Il diritto dell'era digitale

Quali sono i rapporti tra l'odierna tecnologia, informatica e telematica, e il diritto? La tecnologia si fa, per un verso, strumento del diritto, per un altro diviene essa stessa oggetto del diritto, che deve disciplinare fenomeni nuovissimi. Il volume, qui presentato in una nuova edizione aggiornata e ampliata, offre un panorama completo del diritto dell'era digitale illustrando, con ricchezza di riferimenti normativi, le novità legislative, dottrinali e giurisprudenziali intervenute negli ultimi anni.

GIOVANNI PASCUZZI insegna Diritto civile nell'Università di Trento. Tra i suoi libri: «Diritto e tecnologie evolute del commercio elettronico» (2004); «Cyberdiritto 2.0. Guida alle banche dati italiane e straniere, alla rete Internet e all'apprendimento assistito da calcolatore» (2003); «Diritto e informatica» (2002); «I diritti sulle opere digitali. Copyright statunitense e diritto d'autore italiano» (2002, a cura di, con R. Caso); «Il diritto fra tomi e bit: generi letterari e ipertesti» (1997). Per il Mulino ha pubblicato anche «Giuristi si diventa. Come riconoscere e apprendere le abilità proprie delle professioni legali» (2008).

All'indirizzo **www.mulino.it/aulaweb** docenti e studenti troveranno materiale utile alla didattica e all'apprendimento.

Terza edizione aggiornata

ISBN 978-88-15-13878-1

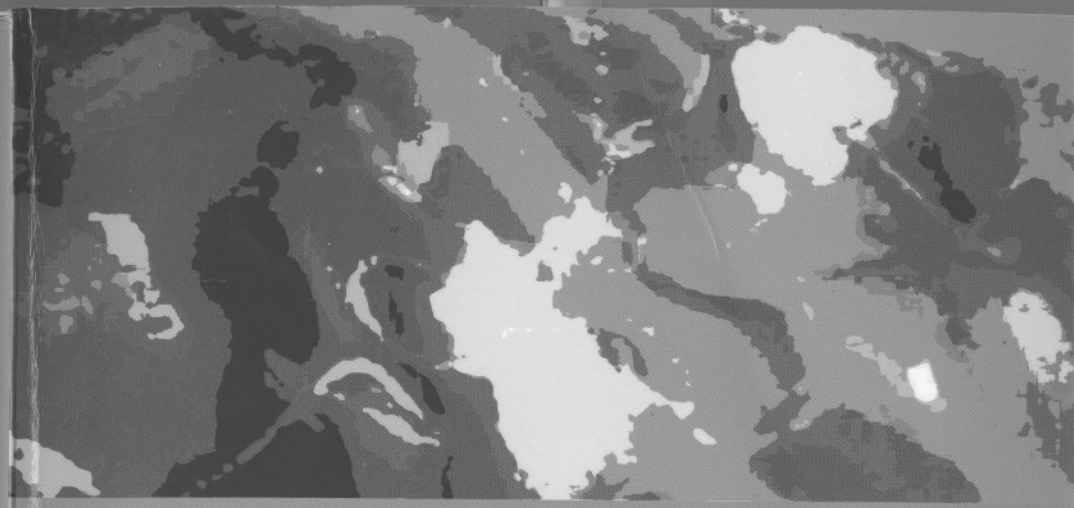
9 788815 138781

€ 24,00

Progettazione grafica: Francesca Vaccari

PASCUZZI

Il diritto dell'era digitale



GIOVANNI PASCUZZI

Il diritto dell'era digitale

aulaweb

il Mulino Itinerari

a mia madre Lella

GIOVANNI PASCUZZI

Il diritto dell'era digitale

il Mulino

I lettori che desiderano informarsi sui libri e sull'insieme delle attività della Società editrice il Mulino possono consultare il sito Internet:
www.mulino.it

ISBN 978-88-15-13878-1

Indice

Introduzione

1. IL PUNTO DI PARTENZA

Esiste un rapporto molto stretto tra diritto e tecnologia[1]. Più in particolare esiste una relazione simbiotica tra il diritto e le attività umane che, sfruttando le acquisizioni della scienza, creano nuovi mezzi, strumenti, congegni, apparati atti a migliorare le condizioni di vita dell'uomo stesso [Rodotà 1995].

Il rapporto tra diritto e tecnologia appare evidente quando si affrontano temi quali la fecondazione artificiale o la brevettabilità di nuove specie animali o vegetali. Anche la rivoluzione informatica impone all'esperienza giuridica di misurarsi con un retroterra tecnologico.

Il clamore suscitato dalle innovazioni induce a credere che il rapporto diritto/tecnologia sia caratteristico delle epoche a noi più recenti. Si finisce così per non prestare abbastanza attenzione al fatto che il diritto è sempre stato in relazione con le tecnologie. In un libro che narra la storia della scrittura [AA.VV. 2000, 8] si legge testualmente: «la scrittura nasce in forma pittografica e ideografica per *documentare* i raccolti, la *proprietà* degli animali, il *patrimonio* della casta sacerdotale».

In tre righe compaiono le parole *documentare*, *proprietà*, *patrimonio*: concetti, attività, istituti che fanno parte dell'armamentario quotidiano del

[1] I siti Internet citati nel libro si intendono visitati nel mese di febbraio 2010.

giurista. Insomma, a dar retta a quelle righe, la scrittura (tra i primi ritrovati tecnologici) è stata inventata dall'uomo per perseguire obiettivi (ad esempio la documentazione) fondamentali per il diritto. Attraverso quell'invenzione è stato più facile fondare (e far rispettare) istituti come la proprietà.

Oggi l'attenzione è attirata dalle tecnologie digitali. Ma a ben vedere i bit, i programmi, i computer non sono più tecnologia di quanto non lo siano la carta, la penna o lo stesso linguaggio (tecnologia del pensiero) [Pascuzzi 1996; 1997].

Per convincersene bastano alcuni esempi. La nostra civiltà ha interiorizzato le parole e la scrittura (strumenti di attività grandiose come la rappresentazione del pensiero e la descrizione del mondo intorno a noi) al punto da dimenticare che esse sono invenzioni e tecnologie tipiche di un periodo molto piccolo della storia dell'uomo [Ong 1989]. All'armamentario tecnologico è da ricondurre anche il materiale scrittorio (primariamente: la carta) che consente alla scrittura di mantenersi stabile nel tempo e di poter circolare nello spazio. Come ben si vede, si sta parlando delle invenzioni e delle tecnologie ad esse connesse che hanno consentito all'uomo di affrancarsi dalla preistoria.

Le tecnologie connesse alla scrittura (come, nel caso ricordato, il materiale su cui si scrive) svolgono un ruolo rilevantissimo nel garantire (tra l'altro) certezza e stabilità, due requisiti vitali per le relazioni giuridiche (ad esempio contrattuali). Quando non esisteva la scrittura o quando ancora diffuso era l'analfabetismo, i testimoni (e, quindi, la memoria orale) rappresentavano lo strumento utilizzato per dare certezza ai traffici giuridici e stabilità agli atti che venivano compiuti e ai fatti che si verificavano[2].

Una società senza alfabeto, parole, scrittura e carta in abbondanza avrebbe un diritto molto diverso da quello che oggi conosciamo. E la nostra storia è lì a rammentarlo.

La compilazione del *Domesday Book* viene ancora oggi ricordata come esempio della capacità amministrativa dei Normanni[3]. In quel caso la dispo-

[2] Per un'efficace illustrazione di come l'oralità incideva sul modo di essere dell'esperienza giuridica inglese tra i secoli XI e XIV cfr. Clanchy [1979].

[3] Cfr. Cannata e Gambaro [1989, 34]: «Manifestazione evidente della capacità amministrativa dei Normanni fu la compilazione del *Domesday Book*, un libro del catasto ordinato da Guglielmo (il Conquistatore) nel 1085 e realizzato l'anno successivo. Furono registrati con scrupolo non solo tutti gli abitanti, ma tutte le ricchezze materiali del regno. La compilazione del *Domesday Book* aveva ovviamente scopi fiscali e la celerità, la cura e la precisione con cui fu portato a termine scioccarono i contemporanei».

nibilità delle tecnologie appena ricordate consentì (e ha poi consentito per secoli) di perseguire obiettivi di natura fiscale vitali per la nascita e la sopravvivenza di comunità organizzate (nei tempi più recenti, prevalentemente nella forma Stato)[4].

In sintesi, questo libro muove dai seguenti assunti:

– esiste un rapporto stretto tra diritto e tecnologie;

– il diritto è chiamato a disciplinare le tecnologie, ma al tempo stesso si serve di tecnologie per perseguire fini suoi propri;

– oggi l'attenzione è attirata dalle tecnologie digitali, ma occorre prestare attenzione al fatto che hardware, software e reti telematiche non sono «più tecnologia» di quanto lo siano la carta, la penna o lo stesso linguaggio (tecnologia del pensiero);

– le regole giuridiche, in quanto perseguono obiettivi servendosi delle tecnologie disponibili nel momento in cui vengono create, sono legate a filo doppio alle tecnologie che ne hanno propiziato e favorito la creazione;

– nel momento in cui il progresso mette a disposizione dell'uomo nuove tecnologie è verosimile che queste ultime possano essere usate dal diritto per perseguire propri obiettivi (vecchi e nuovi), con la conseguenza che l'avvento di nuove tecnologie può portare alla creazione di nuove regole.

2. GLI OBIETTIVI DEL LIBRO

Se si osserva l'evoluzione del diritto in chiave diacronica è facile rendersi conto che svolte epocali si sono verificate ogniqualvolta l'uomo ha avuto accesso a nuove tecnologie. L'evoluzione del diritto coincide anche con l'evoluzione dei mezzi espressivi e delle tecnologie connesse a questi ultimi [Pascuzzi 1997]. Proviamo a fare qualche esempio.

[4] Cfr. Criscuoli [1981, 88]: «Il mezzo tecnico che consentì di avere un quadro completo delle risorse del paese fu il c.d. *Domesday Book* [...]. Per la sua completezza il *Domesday Book* rappresentò ben più che un testo di carattere fiscale. Servì, difatti, ottimamente ad altri fini: militari, giudiziari, di polizia e propriamente amministrativi, consentendo la ripartizione del territorio sulla base dell'unità locale costituita dalla contea alle dipendenze di uno sceriffo».

Quando l'uomo si esprimeva solo a gesti, il diritto (definito muto) si caratterizzava per l'assenza di qualsivoglia forma di concettualizzazione[5].

Con il tempo assistiamo alla prima innovazione tecnologica: la disponibilità del linguaggio articolato (tecnologia del pensiero). Il diritto cambia ed evolve. Nelle società senza scrittura il patrimonio giuridico viene consegnato alle generazioni successive in forma orale[6]. E questo comporta l'impossibilità di discorsi complicati, esclude l'astrazione e la generalizzazione, implica, piuttosto, l'uso di formule brevi e ripetitive[7].

Passano i millenni e l'uomo inventa la scrittura (tecnologia della parola). Il diritto evolve ulteriormente[8]. Il testo (che riproduce la regola) diviene fisso e può essere conservato inalterato. Nasce l'interpretazione.

Un'ulteriore svolta figlia dell'innovazione tecnologica si ha con l'introduzione dei caratteri a stampa. L'invenzione di Gutenberg favorisce la diffusione spaziale dello scritto [McLuhan 1991; Eisenstein 1985; Ong 1989]. Consente

[5] Sacco [1994, 687 e 697] scrive: «Cerimonia e attuazione erano gli atti giuridici. E la fedeltà alla regola implicava l'esistenza e la validità della regola (inducibile dalla spontanea condotta dei membri del gruppo). Il diritto era muto (si prescinde dalle grida che possono aver accompagnato le cerimonie e l'autotutela). Le fonti erano mute. Gli atti erano muti. [...] Il diritto muto non poté battezzare gli istituti giuridici che, già allora, sorreggevano la società e ne condizionavano la sopravvivenza. Non poté battezzarli perché era muto. Ma andò di pari passo con la mancata verbalizzazione la mancata concettualizzazione».

[6] Dopo aver dimostrato che l'uso di frasi fatte (come sono le formule) caratterizza il pensiero che si organizza oralmente, tipico delle società senza scrittura, Ong [1986, 64] scrive: «Nelle culture orali la legge stessa è custodita in massime formulaiche e in proverbi, che non sono mere decorazioni della giurisprudenza, ma costituiscono essi stessi la legge. In una cultura di tipo orale, il giudice viene spesso chiamato ad articolare una serie di proverbi di rilievo, in base ai quali egli ricava giuste decisioni per i casi discussi in sua presenza».

[7] Schiavone [1988, 146] scrive: «La prima "specializzazione" del sapere giuridico deve essersi formata a Roma intorno a consuetudini verbali della collettività, custodite dai pontefici, e divenute, attraverso il filtro della memoria, "tecniche verbali" delle relazioni interpersonali. Come possiamo facilmente supporre, la memorizzazione si realizzava attraverso l'ampio ricorso a elementi formulaici, che di volta in volta potevano essere più o meno fissi e morbidi. Il pensiero doveva conservarsi all'interno di moduli bilanciati, a forte contenuto ritmico. Ed è per questo che tutto il sapere giuridico arcaico appare nella sensibilità più tarda, alla fine della repubblica, come una conoscenza interamente prigioniera di una (ormai) insopportabile armatura di clausole pietrificate». Utile appare anche ricordare un inciso di Sacco [1992, 442]: «i popoli cosiddetti "senza scrittura" possono non avere regole verbalizzate, e in ogni caso, non hanno raccolte di giurisprudenza né opere dottrinali».

[8] Il passaggio dal diritto non scritto al diritto scritto è così raccontato da Stein [1987, 89]: «Quando la scrittura si fa strada, sorge il problema se il diritto consuetudinario debba essere messo per iscritto. Affidare le leggi ad atti scritti ha determinate conseguenze. [...] La redazione delle leggi provoca un distacco del precetto giuridico dai fatti del caso e lo rende così più generale ed astratto [...]. La semplice esistenza di un testo delle leggi apre lo spazio ad analisi ed interpretazioni impensabili, inesistenti quando il diritto non era scritto, e cioè favorisce una nuova classe di esperti [...]. Il diritto tende a divenire più tecnico».

la stabilizzazione e la standardizzazione dei testi e del linguaggio. Costituisce la premessa perché si pongano in essere concettualizzazioni e astrazioni. Insieme ad una classe di esperti, nasce una tradizione giuridica colta[9].

L'analisi diacronica dimostra che ogni stadio evolutivo deriva alcune sue peculiarità dalle caratteristiche delle tecnologie adoperate. Il diritto dei popoli primitivi (c.d. diritto muto) è diverso da quello delle società orali che ancora non conoscono la scrittura. Così come la cultura giuridica che si produce attraverso un'ampia utilizzazione della stampa (libri, collane, riviste, ecc.) è molto diversa da quella che poteva contare su rari manoscritti.

È allora possibile formulare una domanda: se la storia dimostra che il diritto ha subito importanti evoluzioni ogniqualvolta l'uomo ha avuto a disposizione nuove tecnologie per rappresentare, conservare e diffondere il pensiero (giuridico), oggi che sulla scena irrompe la tecnologia digitale, è lecito attendersi un cambiamento del diritto?

Diventa così fondamentale saper cogliere cosa, di una certa evoluzione, è dovuto alle caratteristiche proprie di una singola tecnologia. La sfida, in questo momento, è rappresentata dalle tecnologie digitali. Così, se è utile chiedersi in che modo il diritto disciplina i fenomeni legati all'informatica e alla

[9] Febvre e Martin [1988, 7] scrivono: «Definire la posta in gioco, stabilire come e perché il libro a stampa sia stato ben altro che una realizzazione tecnica, comoda e ingegnosamente semplice, ma la messa a punto di uno degli strumenti più potenti di cui abbia disposto la civiltà occidentale per raccogliere il pensiero sparso dei suoi rappresentanti e conferire tutta la forza possibile alla meditazione individuale dei ricercatori, trasmettendola anche ad altri; riunire a proprio piacere, senza indugio e fatica e spesa, quel concilio permanente di grandi spiriti di cui parlò Michelet in termini imperituri; conferirgli una forza centuplicata, una coerenza tutta nuova, e, quindi, un'incomparabile forza di penetrazione e di irradiazione; assicurare in brevissimo tempo la diffusione delle idee là dove non era ostacolata da difficoltà di lingua o di scrittura, creare inoltre, negli intellettuali e al di là della loro stretta cerchia, in tutti coloro che si valgono dell'intelletto, nuove abitudini di lavoro mentale, insomma mostrare nel libro uno dei mezzi più efficaci di quest'egemonia sul mondo». Eisenstein [1999, 56] scrive: «L'era del glossatore e del commentatore giunse al termine e cominciò una nuova "era di articolati rimandi tra un libro e l'altro" [Hay 1958]. [...] Scaffali più pieni aumentavano ovviamente le possibilità di consultare e paragonare testi diversi [...] Le contraddizioni diventarono più visibili; le tradizioni divergenti più difficili da conciliare [...]. Se da un lato si indeboliva la fiducia nelle vecchie teorie, dall'altro un più ricco materiale di lettura incoraggiava lo sviluppo di nuove combinazioni e permutazioni intellettuali [...]. L'attività intellettuale combinatoria [...] ispira molti atti creativi. Una volta che i vecchi testi furono raccolti nello stesso studio, si poterono combinare insieme sistemi diversi di idee e discipline particolari. In breve, la maggior produzione rivolta a mercati relativamente stabili dapprima creò le premesse per nuove combinazioni di vecchie idee e quindi, successivamente, portò alla creazione di sistemi di pensiero completamente nuovi [...]. La stampa incoraggiò forme di attività combinata tanto sociali quanto intellettuali. Cambiò i rapporti tra gli uomini di cultura oltre che tra i sistemi di idee. Lo scambio culturale incrociato stimolò le attività mentali in tutte le direzioni».

telematica, è indispensabile anche chiedersi se e in che modo quelle tecnologie stanno cambiando (oltre a tante altre cose) il fenomeno giuridico. È verosimile che l'utilizzo dei bit incida sugli stessi contenuti culturali e operazionali.

L'ultima affermazione circoscrive il raggio d'azione del presente lavoro. Il rapporto diritto-tecnologie ha contenuti variegati [Jasanoff 2001]. In questa sede si prenderà in esame la relazione tra diritto e tecnologie informatiche muovendo dall'assunto che l'uso dell'informatica e della telematica è in grado di cambiare il diritto.

Quest'ultima affermazione ha una valenza almeno duplice. Il diritto cambia perché le regole operazionali devono adeguarsi ai mutamenti della realtà ovvero perché la costruzione e la rappresentazione della riflessione giuridica obbediscono a paradigmi differenti.

Un precedente lavoro ha scandagliato la seconda tra le valenze indicate [Pascuzzi 1997]. Questo volume si propone di analizzare i cambiamenti che l'era digitale è suscettibile di produrre nelle regole operazionali.

In sintesi, questo libro si propone di:

– verificare se e in che modo le tecnologie informatiche stanno cambiando le regole (operazionali) giuridiche, attraverso l'esame concreto di istituti quali: la tutela della riservatezza, la documentazione, la sottoscrizione, i titoli di credito, la pubblicità immobiliare, i mezzi di pagamento, il contratto, il diritto d'autore;

– cercare di capire se l'eventuale emersione di nuove regole in ragione dell'avvento delle tecnologie informatiche coincida con l'emersione di tratti caratteristici comuni che possano indurre a parlare di diritto dell'era digitale.

3. CHE COSA SIGNIFICA «ERA DIGITALE». CONVERGENZA TECNOLOGICA E PRINCIPIO DI NEUTRALITÀ

Al fine di chiarire meglio i fenomeni di cui si discute è utile formulare alcune premesse terminologiche.

Il termine «digitale» è un anglicismo[10]: in inglese *digit* vuol dire «numero». L'espressione «digitale», quindi, individua un segnale, una misurazione o una rappresentazione di un fenomeno attraverso numeri[11]. Esistono vari sistemi di numerazione [Burrow 1992]; quello a noi più familiare è il sistema decimale. La scrittura dei numeri che usiamo è denominata «notazione posizionale in base 10» [Lolli 1996, 39]. La scrittura dei numeri in base 2, in cui esistono solo le cifre 0 e 1, è la notazione posizionale più semplice ed essenziale e viene definita sistema binario. La locuzione «carattere binario» traduce l'inglese *binary digit*. Dalla crasi di questi due termini è nato il termine *bit*.

Nella notazione in base 2 è implicita la logica binaria (c'è o non c'è, acceso o spento, vero o falso). Proprio per questo essa è cara agli informatici. La logica binaria è quella con cui vengono registrati i dati (tutti i dati, anche quelli più complessi e apparentemente lontani dai numeri) all'interno del calcolatore. Possiamo descrivere la memoria della macchina come composta da un numero elevatissimo di celle, ciascuna delle quali contiene a sua volta dei dispositivi binari (immaginabili come microscopiche lampadine) capaci di due stati (acceso/spento, sì/no). Ogni informazione, anche la più elaborata, può essere ridotta a una sequenza di 0 e di 1.

L'utilizzo massivo della notazione binaria e della logica ad essa sottesa sta segnando la nostra epoca, oggi comunemente definita era digitale. Quest'ultima locuzione riassume fenomeni ben precisi che di seguito verranno richiamati al fine di delineare il quadro di riferimento entro cui ci si muove.

a) Rappresentazione. La tecnologia digitale consente di rappresentare tutte le forme espressive (testi, suoni, immagini) in notazione binaria. Molte delle cose che oggi siamo abituati a immaginare come indissolubilmente connesse a un elemento materiale possono essere ridotte a sequenze di numeri utilizzando un codice (comune) binario. Un testo letterario[12], l'imma-

[10] L'origine è comunque latina: *digitus* «dito» (che serve per numerare). Cfr. la definizione della parola «digitale» offerta dal vocabolario della lingua italiana Zingarelli.

[11] In termini più generali occorrerebbe parlare di rappresentazione di un fenomeno espressa in elementi discreti. Discreto è sinonimo di discontinuo (fenomeno di cui è possibile individuare le parti). In questo senso il termine «digitale» è contrapposto al termine «analogico» (non discreto). Sono analogici i dispositivi che trattano grandezze rappresentate da altre grandezze legate alle prime da una relazione di analogia.

[12] Molti editori di opere a stampa stanno realizzando archivi digitali dei libri cartacei. Il Mulino, ad esempio, ha varato il progetto «Darwinbooks» (http://www.darwinbooks.it/main) per rispondere alle nuove esigenze di ricerca e studio dell'università italiana. La società editrice propone in rete centinaia di monografie pubblicate a stampa dopo il 2000. I volumi, collocati in collezioni disciplinari, sono consultabili a partire dall'indice, dal quale si ha accesso ai capitoli, ai paragrafi, agli

gine di un quadro o di una fotografia, il suono di uno strumento musicale, la voce di un cantante lirico sono solo esempi di fenomeni espressivi digitalizzabili ovvero rappresentabili come sequenze di informazioni (bit = unità minima di informazione).

b) *Elaborazione*. Il codice binario (e quindi le informazioni in esso racchiuse) può essere facilmente trattato ed elaborato grazie a strumenti automatici come i computer (non a caso il termine «informatica» nasce dalla crasi dei termini francesi *information* e *automatique*).

c) *Comunicazione*. L'era digitale, infine, si caratterizza per la convergenza tra le tecnologie informatiche e le tecnologie della comunicazione (ancora una volta è una parola ad evocare una realtà: il termine «telematica» deriva dall'unione delle parole «telecomunicazione» e «informatica»). Grazie alle reti di calcolatori, i bit (elaborati) possono viaggiare trasferendo informazioni da una parte all'altra del globo in tempi ridottissimi.

Sul terzo degli elementi indicati come caratterizzanti l'era digitale conviene soffermarsi perché ha assunto grande rilevanza qualitativa e quantitativa, sì da risultare centrale nel quadro che si sta descrivendo.

Le tecnologie tradizionali (di derivazione analogica) avevano modellato uno scenario caratterizzato da una netta distinzione tra infrastrutture, servizi e corrispondenti contenuti. Il telefono era il terminale di un'apposita rete e forniva un determinato tipo di servizio connesso alla comunicazione. Dal canto loro la radio e la televisione erano i terminali di altre reti utili a fornire un diverso tipo di servizio. Esisteva una ferrea coincidenza tra mezzo (piattaforma) e servizio che lo stesso consentiva di trasmettere, coincidenza che si risolveva, sul piano giuridico, nello sviluppo di discipline differenziate per i diversi mezzi trasmissivi (specchio di tale impostazione era il codice postale e delle telecomunicazioni, emanato con d.p.r. 29 marzo 1973, n. 156, che distingueva tre tipi di servizi: telegrafia, telefonia, radiocomunicazioni).

apparati. Sul singolo titolo e sull'archivio nel suo complesso sono possibili ricerche nei dati bibliografici, ma anche nel testo completo o in sue parti specifiche (ad esempio, solo le figure, le tabelle, le note, la bibliografia, ecc.). I lettori possono trarre citazioni testuali complete di dati bibliografici, inserire appunti personali a commento di parole o frasi, esportare i riferimenti più significativi nei principali *social networks*. Ogni libro e ogni capitolo sono contraddistinti da un DOI (*Digital object identifier*), per un riferimento rapido e univoco in rete. Esistono anche altre iniziative simili. Si veda, ad esempio, *Scrittori d'Italia* all'indirizzo http://www.bibliotecaitaliana.it/ScrittoriItalia/catalogo/index.xml. Google, il noto motore di ricerca, ha varato un ambizioso progetto di digitalizzazione dei contenuti di tutti i libri editi nel mondo (http://books.google.com/). Sull'iniziativa si tornerà nel capitolo dedicato al diritto d'autore.

La rivoluzione digitale sta profondamente cambiando questo scenario: la telematica, le reti a fibra ottica e satellitari su cui viaggiano i segnali numerico-digitali, le tecniche di compressione[13] e codifica[14] degli stessi, sono tutte innovazioni che stanno annacquando notevolmente fin quasi a farla scomparire la distinzione tra telefono, televisore e computer. Oggi su uno stesso apparecchio, terminale di una medesima rete, si può ricevere una pluralità di servizi un tempo rigidamente distinti (si pensi alla possibilità di vedere i programmi televisivi sul telefono cellulare ovvero alla possibilità di usare il televisore come terminale telematico).

Si sta assistendo ad un fenomeno di «convergenza tecnologica» che comporta precise ricadute sul piano giuridico ed economico[15]. Si consideri l'appannamento della distinzione tra gli artt. 15 e 21 della Costituzione. Alla prima delle citate disposizioni si è tradizionalmente fatto riferimento allorché si sono dovuti individuare i principi in materia di telecomunicazioni tra soggetti predefiniti per quel che attiene, ad esempio, la libertà e la segretezza della corrispondenza. L'art. 21 tutela, invece, le manifestazioni di pensiero rivolte ad un pubblico indeterminato[16]. A quale delle due categorie di comunicazione devono essere ricondotti fenomeni resi possibili dalle nuove

[13] Le tecniche di compressione consentono di ridurre la quantità di bit necessari alla rappresentazione in forma digitale di un'informazione: per questa via è possibile trasmettere grandi volumi di informazioni (si pensi ad un film in formato digitale) senza bisogno di avere reti di ampia capacità. Esistono tecniche, di regola corrispondenti ad altrettanti standard, che comprimono i dati sfruttando le ridondanze nel loro utilizzo producendo, però, perdite d'informazione (ad esempio: la qualità di un video). Altre tecniche, invece, sfruttano le ridondanze nella codifica dei dati restituendoli senza perdita di informazione. Esempi del primo tipo sono i formati: MP3, MPEG-1, MPEG-2, MPEG-4, DivX. Alle tecniche del secondo tipo sono riconducibili i formati: Zip e Rar.

[14] La codifica di un segnale altera le caratteristiche dello stesso per renderlo più adatto ad una determinata applicazione. ASCII (acronimo di *American standard code for information interchange*) è, ad esempio, un sistema di codifica dei caratteri comunemente utilizzato nei calcolatori.

[15] Già nel 1997 la Commissione europea aveva pubblicato il Libro verde sulla convergenza tra i settori delle telecomunicazioni, dell'audiovisivo e delle tecnologie dell'informazione e sulle sue implicazioni normative nel quale si legge: «Il termine "convergenza" sfugge a una definizione precisa ma viene di solito indicata come: *a*) la capacità di differenti piattaforme di rete di gestire servizi di tipo fondamentalmente simile, o *b*) l'unificazione di apparecchiature di largo consumo (ad esempio telefono, televisione e computer)».

[16] Corte cost., 15 novembre 1988, n. 1030, in «Foro it.», 1989, I, c. 347 aveva chiarito che «l'essenziale distinzione tra i diritti di libertà garantiti dagli artt. 15 e 21 Cost. si incentra effettivamente sull'essere la comunicazione, nella prima ipotesi, diretta a destinatari predeterminati e tendente alla segretezza e, nell'altra, rivolta invece ad una pluralità indeterminata di soggetti».

tecnologie (e su cui si tornerà nel prosieguo) come la *Pay tv*, le *chat lines*, le *mailing lists* e i *newsgroups*?[17]

Per quel che riguarda, poi, il profilo economico si deve considerare che in passato i servizi di telecomunicazione erano gestiti da imprese pubbliche in regime di monopolio[18]. L'innovazione tecnologica ha consentito di superare le caratteristiche che portavano a configurare le telecomunicazioni come monopolio naturale rendendo concretamente possibile l'accesso ad una pluralità di operatori con conseguente liberalizzazione dei mercati[19].

Le ricadute sul piano normativo di queste innovazioni tecnologiche si sono avute grazie soprattutto all'intervento dell'Unione europea che si è mossa sin dall'inizio degli anni '90 del secolo scorso con una serie di importanti direttive. Ai fini del presente lavoro conviene ricordare che tale intervento ha avuto un passaggio decisivo nel 2002 con l'emanazione di un pacchetto di direttive, in parte modificate nel dicembre del 2009. Tali direttive sono:

[17] Caretti [2004, 212] scrive: «proprio muovendo dalla considerazione delle caratteristiche che presentano quelle forme comunicative che si collocano su un terreno di interferenza tra le due libertà costituzionali in questione, della pluralità di funzioni cui esse assolvono, si è proposta una interpretazione che riconduce le due libertà ad un'unica matrice (quella di assicurare a tutti la libertà di comunicare ad altri il proprio pensiero attraverso qualunque mezzo; quella che è chiamata libertà di comunicazione) differendo il grado di tutela essenzialmente in ragione delle concrete modalità comunicative prescelte, idonee o meno a trasmettere messaggi informativi a singoli o alla generalità (verifica questa da farsi caso per caso e non predeterminabile *a priori*)».

[18] Cfr. l'ormai superato art. 1, d.p.r. 156/1973.

[19] Il processo di convergenza tecnologica ha convinto il legislatore italiano dell'opportunità di affidare ad un unico organismo le funzioni di regolamentazione e vigilanza nei settori delle telecomunicazioni, dell'audiovisivo e dell'editoria. Si tratta della Autorità per le garanzie nelle comunicazioni (AGCOM) istituita con la legge 31 luglio 1997, n. 249 (http://www.agcom.it). L'Autorità ha il duplice compito di assicurare la corretta competizione degli operatori sul mercato e di tutelare i consumi e le libertà fondamentali dei cittadini. In particolare le garanzie riguardano: *a*) gli operatori, attraverso l'attuazione della liberalizzazione nel settore delle telecomunicazioni, con le attività di regolamentazione e vigilanza e di risoluzione delle controversie; la razionalizzazione delle risorse nel settore dell'audiovisivo; l'applicazione della normativa antitrust nelle comunicazioni e la verifica di eventuali posizioni dominanti; la gestione del Registro unico degli operatori di comunicazione; la tutela del diritto d'autore nel settore informatico ed audiovisivo; e *b*) gli utenti, attraverso: la vigilanza sulla qualità e sulle modalità di distribuzione dei servizi e dei prodotti, compresa la pubblicità; la risoluzione delle controversie tra operatori e utenti; la disciplina del servizio universale e la predisposizione di norme a salvaguardia delle categorie disagiate; la tutela del pluralismo sociale, politico ed economico nel settore della radiotelevisione. La legge 249/1997 (art. 1, comma 28) ha anche istituito il Consiglio nazionale degli utenti e previsto (art. 1, comma 13) la costituzione, attraverso leggi regionali, di articolazioni decentrate dell'Autorità denominate Comitati regionali per le comunicazioni (CORECOM) [Caretti 2004, 195].

a) direttiva 2002/21/CE del Parlamento europeo e del Consiglio del 7 marzo 2002 che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (direttiva quadro) modificata dalla direttiva 2009/140/CE del Parlamento europeo e del Consiglio del 25 novembre 2009[20];

b) direttiva 2002/20/CE del Parlamento europeo e del Consiglio del 7 marzo 2002 relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica (direttiva autorizzazioni), modificata dalla direttiva 2009/140/CE del Parlamento europeo e del Consiglio del 25 novembre 2009;

c) direttiva 2002/19/CE del Parlamento europeo e del Consiglio del 7 marzo 2002 relativa all'accesso alle reti di comunicazione elettronica e delle risorse correlate nonché all'interconnessione delle stesse (direttiva accesso) modificata dalla direttiva 2009/140/CE del Parlamento europeo e del Consiglio del 25 novembre 2009;

d) direttiva 2002/22/CE del Parlamento europeo e del Consiglio del 7 marzo 2002 relativa al servizio universale e ai diritti degli utenti in materia di reti e servizi di comunicazione elettronica (direttiva servizio universale), modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009;

e) direttiva 97/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, abrogata e sostituita dalla direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009.

Si veda, da ultimo, anche il regolamento CE 1211/2009 del Parlamento europeo e del Consiglio del 25 novembre 2009 che istituisce l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC) e l'Ufficio.

[20] La direttiva 2002/21/CE era stata emendata anche dal regolamento CE 717/2007 del Parlamento europeo e del Consiglio del 27 giugno 2007 e dal regolamento CE 544/2009 del Parlamento europeo e del Consiglio del 18 giugno 2009.

Le ragioni dell'intervento comunitario sono efficacemente sintetizzate nel considerando n. 5 della direttiva 2002/21/CE del Parlamento europeo e del Consiglio del 7 marzo 2002 che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (direttiva quadro) che così recita:

> La convergenza dei settori delle telecomunicazioni, dei media e delle tecnologie dell'informazione implica l'esigenza di assoggettare tutte le reti di trasmissione e i servizi correlati ad un unico quadro normativo [...]. È necessario separare la disciplina dei mezzi di trasmissione dalla disciplina dei contenuti. Di conseguenza, il presente quadro normativo non si applica ai contenuti dei servizi forniti mediante reti di comunicazione elettronica che utilizzano servizi di comunicazione elettronica, come i contenuti delle emissioni radiotelevisive, i servizi finanziari e taluni servizi della società dell'informazione e lascia quindi impregiudicate le misure adottate a livello comunitario o nazionale riguardo a tali servizi in ottemperanza alla normativa comunitaria, per promuovere la diversità culturale e linguistica e per assicurare la difesa del pluralismo dei mezzi di informazione[21].

In Italia questo significativo intervento comunitario è stato attuato soprattutto con il d.lgs. 1° agosto 2003, n. 259[22], denominato «codice delle comunicazioni elettroniche» [Clarich e Cartei 2004]; ma si vedano anche il d.lgs. 82/2005 (codice dell'amministrazione digitale); il d.lgs. 177/2005, t.u. dei servizi di media audiovisivi e radiofonici[23] [Frignani, Poddighe e Zeno Zencovich 2006]; il d.lgs. 196/2003 (codice della privacy). Occorre ora attendere l'attuazione delle modifiche introdotte nel 2009.

Tra le innovazioni più significative introdotte dal d.lgs. 259/2003 conviene ricordare:

a) l'inclusione tra le reti di comunicazione elettronica delle reti che trasportano il segnale televisivo. Tale innovazione non incide sulla materia radiotelevisiva, intesa come servizi che forniscono «contenuto» trasmesso utilizzando reti e servizi di comunicazione elettronica o che comportano un controllo editoriale: tali contenuti rimangono disciplinati da apposite norme europee e nazionali;

b) l'assorbimento, per quel che attiene il titolo legittimante lo svolgimento dell'attività, del sistema dualista precedente, articolato in licenze individuali e autorizzazioni generali nel sistema dell'autorizzazione generale che si sostanzia in una denuncia di inizio attività da parte dell'impresa interessata;

c) l'ancoraggio degli obblighi posti a carico degli ex monopolisti, e degli operatori individuati come aventi un significativo potere di mercato, all'esito di un'analisi di mercato e all'individuazione – caso per caso – delle occorrenti misure, commisurate alle distorsioni da eliminare;

d) la tutela di diritti di rango costituzionale quali la libertà di comunicazione, la libertà di iniziativa economica privata e la segretezza delle comunicazioni[24];

[21] Il considerando citato così prosegue: «Il contenuto dei programmi televisivi è disciplinato dalla direttiva 1989/552/CEE del Consiglio del 3 ottobre 1989, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti l'esercizio delle attività televisive. La separazione della disciplina dei mezzi di trasmissione dalla disciplina dei contenuti non incide sul riconoscimento dei collegamenti fra i due aspetti, in particolare al fine di garantire il pluralismo dei mezzi di informazione, la diversità culturale e la protezione dei consumatori». La direttiva 1989/552/CEE è stata modificata con direttiva 2007/65/CE del Parlamento europeo e del Consiglio dell'11 dicembre 2007 (c.d. direttiva sui servizi di media audiovisivi). Per l'attuazione di detta nuova direttiva si veda il d.lgs. 15 marzo 2010, n. 44. La direttiva 1989/552/CEE è stata poi abrogata dalla direttiva 2010/13/UE che si è posta obiettivi di chiarificazione e di razionalizzazione della materia.

[22] Il decreto è stato emanato ai sensi dell'art. 41 della legge 1° agosto 2002, n. 166. Vedi ora l'art. 5 d.lgs. 59/2010.

[23] Le principali modalità di diffusione/commercializzazione dei segnali televisivi attualmente disponibili sono [Corsi 2008]: *Free tv* (FTA), ovvero la televisione tradizionale oggi fruibile in analogico e digitale; *Pay tv*, che consente la fruizione di un canale televisivo verso il pagamento di un corrispettivo (di regola: canone mensile); *Pay per view* (PPV), che consente la fruizione a pagamento di un singolo programma; *Video on demand* (VOD), che permette di fruire di un archivio di programmi messo a disposizione dal *provider* televisivo in qualsiasi momento. L'art. 1, lett. *d*, del codice delle comunicazioni elettroniche definisce le apparecchiature digitali televisive avanzate con queste parole: «sistemi di apparecchiature di decodifica destinati al collegamento con televisori o sistemi televisivi digitali integrati in grado di ricevere i servizi della televisione digitale interattiva». L'art. 21 dello stesso d.lgs. 259/2003 disciplina l'interoperabilità dei servizi di televisione interattiva digitale con l'obiettivo di favorire l'adozione da parte dei fornitori di apparecchiature e dei fornitori di servizi di un'*Application programming interface* (API) aperta. Con quest'ultimo acronimo si intende un'interfaccia software fra applicazioni rese disponibili da emittenti o fornitori di servizi e le risorse delle apparecchiature digitali televisive avanzate per la televisione e i servizi radiofonici digitali (cfr. art. 1, lett. *e*, del codice).

[24] In particolare, secondo quanto disposto dal comma 1, dell'art. 4, d.lgs. 259/2003, «la disciplina delle reti e servizi di comunicazione elettronica è volta a salvaguardare, nel rispetto del principio della libera circolazione delle persone e delle cose, i diritti costituzionalmente garantiti di: *a*) libertà di comunicazione; *b*) segretezza delle comunicazioni, anche attraverso il mantenimento dell'integrità e della sicurezza delle reti di comunicazione elettronica; *c*) libertà di iniziativa economica e suo esercizio in regime di concorrenza, garantendo un accesso al mercato delle reti e servizi di comunicazione elettronica secondo criteri di obiettività, trasparenza, non discriminazione e proporzionalità».

e) l'imposizione alle imprese che forniscono reti e servizi di comunicazione elettronica di obblighi secondo principi di trasparenza, non distorsione della concorrenza, non discriminazione e proporzionalità[25];

f) la garanzia dell'accesso e dell'interconnessione per le reti di comunicazione elettronica a larga banda, nonché della convergenza, interoperabilità tra reti e servizi di comunicazione elettronica e utilizzo di standard aperti, e, ancora, del principio di neutralità tecnologica.

Su quest'ultimo principio conviene spendere qualche parola. Secondo il d.lgs. 259/2003 (art. 4, comma 3, lett. *h*), la disciplina delle reti e servizi di comunicazione elettronica è volta a garantire il rispetto del principio di neutralità tecnologica, inteso come non discriminazione tra particolari tecnologie, non imposizione dell'uso di una particolare tecnologia rispetto alle altre e possibilità di adottare provvedimenti ragionevoli al fine di promuovere taluni servizi indipendentemente dalla tecnologia utilizzata. Peraltro, come si è detto, il legislatore comunitario è intervenuto per emendare il quadro normativo delineato con le direttive che hanno dato origine all'emanazione del d.lgs. 259/2003. In particolare le direttive 2009/140/CE e 2009/136/CE hanno modificato rispettivamente le direttive 2002/21/CE (direttiva quadro) e 2002/22/CE (direttiva servizio universale). La novella ha rimarcato in più punti la necessità di implementare il principio della cosiddetta «neutralità tecnologica». In realtà di questo concetto esistono più definizioni, riconducibili all'idea secondo la quale una rete a banda larga deve essere priva di restrizioni arbitrarie sui dispositivi connessi e sul modo in cui essi operano. Il 18 dicembre 2009 la Commissione ha emanato una Dichiarazione sulla neutralità della rete (GUCE L337 del 2009, p. 69) che così recita:

> La Commissione ritiene che sia della massima importanza conservare l'apertura e la neutralità di Internet, tenendo pienamente conto della volontà dei colegislatori di dichiarare la neutralità della rete come obiettivo politico e principio della regolamentazione che dovrà essere promosso dalle autorità nazionali di regolamentazione[26], rafforzare i correlati requisiti di trasparenza[27] e conferire strumenti di salvaguardia alle autorità nazionali di regolamentazione per prevenire il degrado dei servizi e intralci o rallentamenti del traffico sulle reti pubbliche[28]. La Commissione sorveglierà da vicino l'attuazione di queste disposizioni negli Stati membri, riservando una particolare attenzione al modo in cui sono tutelate le libertà dei cittadini europei sulla rete nella propria relazione sullo stato di attuazione al Parlamento europeo e al Consiglio. Nel frattempo, la Commissione sorveglierà l'impatto degli sviluppi tecnologici e del mercato sulle libertà della rete e riferirà al Parlamento europeo e al Consiglio, entro la fine del 2010, sulla necessità di adottare orientamenti supplementari; farà inoltre ricorso alle proprie competenze nell'ambito della vigente normativa in materia di concorrenza per far fronte alle pratiche anticoncorrenziali che possano insorgere.

[25] Cfr. d.lgs. 259/2003, art. 4, comma 2.

[26] Art. 1, paragrafo 8, lett. *g*, della direttiva 2009/140/CE.

[27] Art. 1, paragrafo 14, della direttiva 2009/136/CE.

[28] Cfr. nota precedente.

È il caso, ora, di approfondire anche su un piano tecnologico la tematica delle reti.

BOX

In particolare: la rete Internet

Una rete di comunicazione può essere definita, in termini estremamente generali, come un sistema che permette di collegare contemporaneamente più di due dispositivi. La rete telefonica è, probabilmente, l'esempio più intuitivo. Quando ad essere collegati tra loro sono gli elaboratori, ci si trova di fronte ad una rete di computer (*computer network*)[29]. Per dialogare tra loro i calcolatori, come gli umani del resto, devono usare un linguaggio comune. In gergo esso è definito come protocollo di comunicazione.

[29] L'art. 1, lett. *dd*, d.lgs. 259/2003 (codice delle comunicazioni elettroniche) definisce le reti di comunicazione elettronica come «i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse, a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato». Si veda nello stesso senso anche l'art. 1, comma 2, lett. *c*, del codice della privacy, e l'art. 2, comma 1, lett. *c* del d.lgs. 177/2005 come sostituito dall'art. 4 del d.lgs. 44/2010.

Normalmente si usa operare una distinzione tra reti locali (o LAN: *Local area network*), che collegano al massimo macchine collocate all'interno di un medesimo edificio, e reti geografiche (o WAN: *Wide area network*), che collegano calcolatori posti in sedi anche molto distanti tra loro. In relazione al parametro della distanza si possono avere: reti regionali, nazionali, internazionali e intercontinentali. Nell'ambito delle reti geografiche le connessioni sono assicurate da linee telefoniche, cavi coassiali, fibre ottiche, onde radio e anche dai satelliti. Gli elaboratori collegati in una rete di questo tipo si chiamano nodi. Un nodo può svolgere funzioni particolari. Può essere, ad esempio, un *server*, vale a dire un computer che gestisce una rete oppure che esegue automaticamente gli ordini che gli vengono inviati da altri computer detti *client*. Il modello *server/client* (nel quale la presenza di un *server* consente a più *client* di condividerne le risorse e le informazioni) è il più diffuso. Un'alternativa è costituita dal modello *peer to peer* (P2P), nel quale il ruolo di *client* e di *server* possono essere scambiati. Esempio di questo approccio si ha nelle reti per la condivisione di file (*file sharing*).

Sono ormai tantissime le reti che interconnettono terminali posti a grande distanza. La regina delle reti è Internet.

Malgrado costituisca la rete più importante e lo strumento per lo scambio di informazioni maggiormente usato, è difficile fornire una definizione esatta di Internet. Si può pensare a Internet come ad una rete di reti che adoperano protocolli di comunicazione comuni, o come una comunità di persone che utilizzano e sviluppano tali network, o ancora come un insieme di risorse che possono essere raggiunte via rete.

Il nucleo originario di Internet viene fatto risalire ad un esperimento intrapreso poco più di 40 anni fa dal Dipartimento della Difesa statunitense che tentò di interconnettere la propria rete, denominata ARPAnet, con alcune reti radio e satellitari. Il progetto aveva scopi militari: creare un network in grado di resistere a danneggiamenti parziali quali, ad esempio, lo scoppio di una bomba in un determinato sito. Di quel progetto originario è rimasta l'idea di fondo: una rete è affidabile se ogni singolo computer può comunicare con tutti gli altri affinché l'informazione giunga comunque a destinazione.

Oggi Internet è un insieme di reti collegate tra loro da protocolli tecnici comuni che consentono agli utenti di una certa rete di comunicare con utenti di un'altra rete ovvero di utilizzare servizi propri di questa[30]. Il protocollo di comunicazione comune di base è denominato TCP/IP, acronimo di *Transmission control protocol/Internet protocol* [Pascuzzi 2003a]. La forza di Internet (rispetto ad esempio alle reti proprietarie) è proprio l'utilizzo di un protocollo (TCP/IP) costituito da un insieme di regole pubbliche, aperte a tutti (c.d. *open system*), che permette l'interconnessione di reti anche molto differenti, indipendentemente dalla tecnologia usata da ogni rete.

[30] L'art. 1, lett. *aa*, d.m. 8 luglio 2005 (recante «requisiti tecnici e i diversi livelli per l'accessibilità agli strumenti informatici») definisce Internet come «rete mondiale di computer basata sulla famiglia di protocolli di comunicazione TCP/IP (*Transmission control protocol/Internet protocol*)».

Protocollo può essere considerato un insieme di regole per comporre dei messaggi e consentire che essi siano scambiati tra due macchine. Il TCP/IP definisce un'unità di trasmissione dati (denominata *datagram*) e le regole da seguire per trasmettere quella unità in una particolare rete.

Sul piano concettuale, Internet si struttura su più livelli: il livello applicativo[31], quello del trasporto[32] e quello della spedizione dei pacchetti[33]. Esiste, infine, il livello della connessione fisica[34]. Per ognuno di questi livelli è necessario stabilire dei protocolli.

Una similitudine può forse spiegare meglio quanto appena detto. Supponiamo che un avvocato debba scrivere una lettera ad un suo collega (livello applicativo). La costruzione del testo avverrà sulla base di un codice comune a chi scrive e chi legge (parole, stile narrativo, ecc.): è il primo protocollo. L'avvocato consegna la lettera al segretario che provvederà a imbustarla e a scrivere sulla busta: «riservato». Si tratta di un messaggio che deve essere recepito dal segretario dell'avvocato destinatario: un altro protocollo comune, quindi, questa volta di secondo livello (si immagini cosa accadrebbe se al posto della parola «riservato» ce ne fosse una incomprensibile per l'altro segretario. Il messaggio verrebbe perso e la cautela di mantenere riservato il contenuto non potrebbe essere osservata). La lettera viene affidata al fattorino che compie le ultime operazioni per la spedizione: terzo protocollo. Quando, grazie al corriere (che corrisponde alle connessioni fisiche della rete), la lettera giunge a destinazione, il fattorino saprà a chi consegnarla, il segretario conoscerà come trattarla, l'avvocato apprenderà il contenuto del messaggio. Ciò avviene perché (e solo se) ognuno usa un protocollo compatibile con quello adoperato al livello corrispondente nell'organizzazione di partenza[35].

[31] *Application layer*: gestisce i dettagli dell'applicazione e fornisce l'interfaccia per gli utilizzatori. Esempi di protocolli di questo tipo sono: FTP, SMTP, TFTP, BOOTP, SNMP, Telnet/Rlogin, NFS, DNS [Rossato 2006].

[32] *Transport layer*: fornisce il *data flow* per il livello applicativo. Esempi di protocolli di questo tipo sono: TCP, UDP.

[33] *Network layer* (ovvero: *IP layer*): gestisce il movimento dei pacchetti (c.d. *routing* e *messaging*). Esempi di protocolli di questo tipo sono: IP, ICMP, IGMP.

[34] *Link layer*: gestisce i dettagli hardware e la connessione fisica nell'interfacciamento con la rete. Esempi di protocolli di questo tipo sono: ARP, RARP.

[35] È una struttura ispirata al principio *end-to-end*: gli strati inferiori sono indipendenti da

Più in dettaglio TCP/IP è una famiglia di protocolli (c.d. *TCP/IP protocol suite*). Tra essi, quelli di base sono:

1) FTP (*File transfer protocol*). È la funzione di Internet che consente di trasferire i file da una macchina all'altra della rete[36].

2) Posta elettronica (*electronic mail* o e-mail). Questa funzione consente di scambiare messaggi, ovviamente in forma elettronica, fra tutti coloro che hanno accesso a Internet[37].

3) HTTP (*Hypertext transfer protocol*). È un protocollo applicativo alla base del funzionamento del World Wide Web ovvero il sistema che consente di navigare tra milioni di siti che offrono informazioni e servizi[38]. L'unità di base del WWW è la homepage da cui si può cominciare la navigazione verso gli altri siti[39].

I servizi disponibili su Internet si moltiplicano di giorno in giorno. Tra i più diffusi si possono ricordare:

quelli superiori con la conseguenza che è possibile apportare migliorie a questi ultimi senza dover necessariamente modificare gli altri livelli.

[36] Per le specifiche dell'FTP cfr. RFC 959. Sul significato della sigla RFC si avrà modo di tornare più avanti.

[37] Per le specifiche dell'e-mail cfr. RFC 821 e 822.

[38] Esiste una sintassi per identificare le risorse della rete. L'acronimo URI (*Uniform resource identifier*) individua una stringa che identifica univocamente una risorsa come un indirizzo web, un documento, un'immagine, un file, un servizio, un indirizzo di posta elettronica, ecc. L'URI più diffuso è denominato URL (*Uniform resource locator*), che indica il protocollo da usare (ad esempio HTTP per WWW come nel caso http://www.mulino.it/aulaweb) e l'indirizzo per raggiungere la risorsa. È possibile anche utilizzare l'URN (*Uniform resource name*), ovvero un URI che identifica una risorsa mediante un «nome» in un particolare dominio di nomi. Ad esempio l'URN urn:isbn:987-88-15-12627-6 è un URI che consente di individuare univocamente un libro mediante il suo nome 987-88-15-12627-6 tra i codici ISBN.

[39] Per accedere a Internet è necessario disporre di una connessione, ovvero: avere l'apparecchiatura elettronica (hardware) che permette la comunicazione e aver stipulato un contratto con un fornitore di connessione (*service provider*: all'indirizzo http://www.aiip.it/ si può trovare il portale degli *Internet providers* italiani). Sul tema si ritornerà nel capitolo dedicato al commercio elettronico. Si definisce «accessibilità web» la capacità di un sito web di rendersi accessibile efficacemente (nell'interfaccia e nel contenuto) da utenti diversi in differenti contesti. Rendere un sito web accessibile significa permettere l'accesso all'informazione contenuta nel sito anche a persone con disabilità fisiche di diverso tipo e a chi dispone di strumenti hardware e software limitati. Sotto quest'ultimo profilo, in particolare, l'art. 2, comma 1, lett. *a*, legge 9 gennaio 2004, n. 4 (recante «Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici») definisce «accessibilità» la capacità dei sistemi informatici, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari. Cfr., altresì, il d.p.r. 1° marzo 2005, n. 74 (recante il regolamento di attuazione della legge 4/2004); il d.m. 8 luglio 2005 (recante «requisiti tecnici e i diversi livelli per l'accessibilità agli strumenti informatici»); nonché il d.m. 30 aprile 2008 (recante «regole tecniche disciplinanti l'accessibilità agli strumenti didattici e formativi a favore degli alunni disabili»). Al tema è dedicato il sito www.pubbliaccesso.it.

a) *Motori di ricerca*. Per reperire informazioni nel web è possibile collegarsi a siti particolari (come Google, Yahoo!, Altavista, Lycos) che ospitano i c.d. «motori di ricerca». Se, ad esempio, si cerca il testo delle decisioni della Corte suprema statunitense, sarà sufficiente digitare le parole «U.S. Supreme Court» nel *form* che avvia la ricerca testuale per vedersi restituire una lista di siti che contengono informazioni sulla Corte suprema. La lista è composta di collegamenti ipertestuali a detti siti. L'utente può seguire i singoli *links*, scorrendo le informazioni di ciascun sito, fino a trovare il materiale desiderato.

b) *Streaming*. Consente di ottenere attraverso la rete un flusso di dati audio/video riproducibile man mano che arriva a destinazione. È un protocollo di questo tipo che ha decretato, ad esempio, il successo di YouTube, il sito web che consente la condivisione di video tra i suoi utenti. YouTube si propone di ospitare video propri di chi li carica. Spesso, però, vengono inseriti senza autorizzazione materiali di terzi come spezzoni di film, spettacoli televisivi e video musicali. Il sito effettua solo una verifica *ex post* del materiale caricato[40].

c) *Podcasting*. Permette di scaricare in modo automatico documenti (generalmente audio o video) chiamati *podcast*, utilizzando un *client* normalmente gratuito definito «aggregatore» o *feed reader*. Esempio di questa realtà è iTunes, il programma sviluppato da Apple per riprodurre e organizzare file multimediali, e per favorire l'acquisto *on-line* di canzoni, video e film attraverso il servizio *iTunes Store*. A differenza dello *streaming*, che è sincrono e *on-line*, il *podcasting* è asincrono e *off-line*.

d) *VOIP*. Attraverso Internet è possibile effettuare chiamate telefoniche grazie alla tecnologia VOIP (*Voice over IP*: voce tramite protocollo Internet)[41]. VOIP identifica i protocolli di comunicazione di strato applicativo che rendono possibile tale tipo di comunicazione[42]. È possibile effettuare chiamate anche

[40] Il successo dell'iniziativa si è accompagnato, in alcuni casi, ad un uso distorto del servizio. Ad esempio, qualcuno ha caricato video ritraenti episodi di bullismo o di sevizie ai danni di soggetti più deboli. Nel 2009 il Tribunale di Monza ha accolto la richiesta di risarcimento danni avanzata da un'insegnante nei confronti dei genitori di un alunno minorenne che aveva inserito su YouTube un video contenenti immagini lesive del suo decoro e della sua reputazione. Il Tribunale di Milano, il 12 aprile 2010, ha condannato tre dirigenti di Google per violazione della legge sulla privacy, per non aver impedito nel 2006 la pubblicazione nel motore di ricerca di un video ritraente un minore disabile picchiato da alcuni compagni di scuola.

[41] L'art. 78, comma 2-*bis*, d.lgs. 82/2005 (codice dell'amministrazione digitale, su cui si tornerà nei prossimi capitoli), introdotto dall'art. 2, comma 591, legge 244/2007, ha imposto a numerose amministrazioni pubbliche di ricorrere ai servizi VOIP. Per le modalità attuative cfr. il d.m. 9 aprile 2009. Cfr. anche l'art. 36, legge 69/2009.

[42] Cfr. anche le delibere dell'AGCOM, nn. 11/06/CIR («Disposizioni regolamentari per la fornitura di servizi VOIP e integrazione del piano nazionale di numerazione») e 649/09/CONS («Avvio di indagine conoscitiva concernente: garanzie dei consumatori e tutela della concorrenza con riferimento ai servizi vocali su protocollo Internet (VOIP) ed al traffico *peer to peer* da rete mobile»).

verso la rete telefonica tradizionale. Sempre più spesso le grandi compagnie telefoniche si servono di questa tecnologia per fornire il servizio ai propri clienti. Un protocollo VOIP proprietario è alla base di Skype, il sistema di videotelefonate e messaggistica istantanea attualmente più diffuso su Internet.

e) *Web radio* e *IPTV*. Via Internet è possibile fruire di trasmissioni radiofoniche e televisive (*Internet protocol television*). Spesso sono le emittenti tradizionali a trasmettere *on-line* il segnale audio e video dei propri programmi. Ma non mancano esperienze di radio e televisioni che trasmettono esclusivamente in rete.

Quanto appena esposto testimonia come la rete sia in continua evoluzione. L'espressione *Web 2.0* segna il passaggio da uno scenario caratterizzato prevalentemente da siti web statici senza alcuna possibilità di interazione con l'utente se non la navigazione tra le pagine, l'uso delle e-mail e dei motori di ricerca, ad uno scenario nel quale si moltiplicano le applicazioni *on-line* che permettono uno spiccato livello di interazione e socializzazione. Esempi di questi applicativi sono:

1) *Web syndication*. L'espressione indica la distribuzione di contenuti o flussi di informazioni in una forma adatta ad essere riutilizzata in ambiti e formati diversi dal sito che li distribuisce. Attraverso appositi lettori, ma anche semplicemente utilizzando *browser* come Mozilla e Explorer, si sottoscrive un *feed* (i più diffusi sono *RSS* e *Atom*): da quel momento in poi appaiono sotto un'apposita icona tutte le novità che intervengono sul sito presso il quale si è fatta la sottoscrizione. Ad esempio questa possibilità è offerta dai siti di informazione, di regola con una piccola icona che appare sulla destra del rigo che contiene l'indirizzo web del sito stesso: cliccando sull'icona si visualizzano sul proprio *browser* tutte le modifiche che intervengono su una certa pagina web.

2) *Rich Internet application*. Le RIA individuano applicazioni web che, pur possedendo caratteristiche e funzionalità di applicativi tradizionali, non necessitano di installazione sul computer dell'utente. A titolo di esempio si può citare il servizio *iGoogle*, che consente di personalizzare la propria pagina web, oppure *Google Maps*.

3) *Social network*. Alcune piattaforme *on-line* offrono la possibilità di creare reti o relazioni sociali attraverso il web. Spesso il sito che offre questo tipo di servizio viene direttamente definito *social network*. Si vedano, ad esempio, Facebook, Myspace e Twitter.

4) *Blog*. Il termine è la contrazione di *web-log*, ovvero «registro». È un sito Internet in cui l'autore pubblica pensieri, opinioni, riflessioni, considerazioni, oltre ad immagini o video.

5) *Chat*. Il termine individua una gamma di servizi che avvengono in tempo reale e che mettono in contatto quasi sempre sconosciuti in forma anonima.

6) *Forum*. A differenza della *chat* è asincrono in quanto i messaggi vengono scritti e letti anche in momenti diversi. La parola può riferirsi all'intera struttura informatica nella quale degli utenti discutono su vari argomenti, a una sua sottosezione oppure al software utilizzato per fornire questa struttura. Intorno ai forum si sviluppano comunità virtuali formate da utenti con interessi comuni. Il concetto può essere espresso anche con termini come *board*, *message board*, *bulletin board*, *gruppo di discussione*, *bacheca*, *newsgroup*[43].

Un'ulteriore frontiera è rappresentata dal tentativo di costruire un ambiente nel quale i computer siano in grado di comprendere meglio i problemi degli utenti così da trovare soluzioni in modo automatico. Si tratta del cosiddetto «web semantico»: l'idea è quella di associare i documenti del web ad informazioni e dati (metadati) che ne specifichino il contesto semantico in un formato adatto all'interrogazione, all'interpretazione e, più in generale, all'elaborazione automatica. In questo modo si darà la possibilità ai computer di aiutarci a trovare velocemente quello che stiamo cercando: informazioni mediche, recensioni di film, libri da acquistare. Per questa via dovrebbero essere possibili anche attività quali la negoziazione dei diritti sulle opere digitali[44].

Da quanto detto emerge chiaramente l'importanza che Internet ha assunto nella vita dei cittadini. La portata dei cambiamenti in atto è sintetizzata nella raccomandazione del Parlamento europeo del 26 marzo 2009 destinata al Consiglio sul rafforzamento della sicurezza e delle libertà fondamentali su Internet, nella quale, tra l'altro, si legge (punto *a*):

> l'evoluzione di Internet dimostra che esso sta diventando uno strumento indispensabile per promuovere iniziative democratiche, un nuovo foro per il dibattito politico (ad esempio, per campagne elettroniche e il voto elettronico), uno strumento fondamentale a livello mondiale per eserci-

[43] La giurisprudenza si è occupata di ipotesi nelle quali messaggi inviati a forum, *mailing list* o *newsgroup* avevano contenuto diffamatorio. Con riferimento al *forum commissi delicti* cfr.: Cass. [ord.], sez. III, 8 maggio 2002, n. 6591, in «Foro it.», 2002, I, c. 1982; Trib. Lecce, 24 febbraio 2001, in «Foro it.», 2001, I, c. 2031. Sotto altro profilo TAR Lazio, sez. I, 15 novembre 2001, n. 9425, in «Trib. amm. reg.», 2001, I, 3126, ha statuito che i destinatari di corrispondenza e messaggi inviati tramite *mailing list* o *newsgroup* con accesso limitato ai possessori dell'apposita password non sono tenuti a vincoli espressi di riservatezza, salvo il caso di specifici obblighi o cautele disciplinati da particolari norme.

[44] Il web semantico poggia su elementi di base rappresentati da linguaggi specifici come: RDF (*Resource description framework*), XML (*Extensible markup language*), XML *Schema* e XML *Signature*. Per maggiori dettagli http://www.w3.org/standards/semanticweb/.

tare la libertà di espressione (ad esempio il *blog*) e per sviluppare attività commerciali, nonché uno strumento per promuovere l'acquisizione di competenze informatiche e la diffusione della conoscenza (*e-learning*); [...] Internet ha anche apportato un numero crescente di vantaggi per persone di ogni età, ad esempio quello di poter comunicare con altri individui in ogni parte del mondo, estendendo in tal modo la possibilità di acquisire familiarità con altre culture e aumentare la comprensione di popoli e culture diversi; [...] Internet ha anche ampliato la gamma delle fonti di notizie a disposizione dei singoli, che possono ora attingere a un flusso di informazioni proveniente da diverse parti del mondo.

Alla luce di considerazioni di questo tipo, la raccomandazione si spinge fino ad auspicare il riconoscimento di un diritto ad Internet. La stessa, al punto *b*), recita infatti:

Internet può rappresentare una straordinaria opportunità per rafforzare la cittadinanza attiva e che, a tale proposito, l'accesso alle reti e ai contenuti costituisce uno degli elementi chiave; si raccomanda che la questione sia ulteriormente sviluppata sulla base del principio che ogni individuo ha il diritto di partecipare alla società dell'informazione e che le istituzioni e le parti interessate a tutti i livelli detengono la responsabilità generale di partecipare a questo sviluppo, lottando contro le due nuove sfide dell'analfabetismo elettronico e dell'esclusione democratica nell'era elettronica.

Conviene ricordare, sotto questo profilo, che il rapporto tra accesso alle reti di comunicazione elettronica e tutela dei diritti e libertà fondamentali è stato enfatizzato in un recente atto normativo comunitario. La direttiva 2009/140 ha emendato la direttiva quadro per le reti e i servizi di comunicazione elettronica (2002/21/CE: cfr. *supra*) per introdurre all'art. 1 del testo originario il comma 3-*bis*, che così recita:

I provvedimenti adottati dagli Stati membri riguardanti l'accesso o l'uso di servizi e applicazioni attraverso reti di comunicazione elettronica, da parte degli utenti finali, devono rispettare i diritti e le libertà fondamentali delle persone fisiche, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto comunitario.

Qualunque provvedimento di questo tipo riguardante l'accesso o l'uso di servizi e applicazioni attraverso reti di comunicazione elettronica, da parte degli utenti finali, che ostacolasse tali diritti o libertà fondamentali può essere imposto soltanto se appropriato, proporzionato e necessario nel contesto di una società democratica e la sua attuazione deve essere oggetto di adeguate garanzie procedurali conformemente alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e ai principi generali del diritto comunitario, inclusi un'efficace tutela giurisdizionale e un giusto processo. Tali provvedimenti possono di conseguenza essere adottati soltanto nel rispetto del principio della presunzione d'innocenza e del diritto alla privacy. Deve essere garantita una procedura preliminare equa ed imparziale, compresi il diritto della persona o delle persone interessate di essere ascoltate, fatta salva la necessità di presupposti e regimi procedurali appropriati in casi di urgenza debitamente accertata conformemente alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Deve essere garantito il diritto ad un controllo giurisdizionale efficace e tempestivo[45].

Nelle pagine che precedono si è provato a riassumere l'insieme di fenomeni riconducibile ad Internet. Ma lo scenario è tutt'altro che definitivo. Una nuova sfida è ormai rappresentata dal passaggio progressivo da una «rete di computer» interconnessi a una «rete di oggetti» interconnessi. Si parla, a questo proposito, di una «Internet degli oggetti»[46]. Già oggi esistono applicazioni riconducibili a questo paradigma. Si pensi all'uso di telefoni cellulari con accesso a Internet, dotati di macchina fotografica e/o che utilizzano tecnologie NFC (*Near-field communication*) e che consentono agli utenti di avere accesso a informazioni supplementari; ovvero alla tracciabilità di prodotti farmaceutici e di consumo (utile a combattere la contraffazione e la diffusione di prodotti non sicuri); o ancora all'utilizzo da parte di società di servizi del settore energetico di sistemi intelligenti di misurazione dell'elettricità così da fornire ai consumatori infor-

[45] In argomento si vedano anche l'art. 3, comma 1, d.lgs. 259/2003, e l'art. 1, comma 3, della direttiva 2002/22/CE.

[46] Si tratta di oggetti che talora disporranno del proprio indirizzo IP (*Internet protocol*), saranno inseriti in sistemi complessi e utilizzeranno sensori per ottenere informazioni dal proprio ambiente (ad esempio, prodotti alimentari che registrano la temperatura in ogni fase della catena dell'approvvigionamento) e/o dispositivi di comando per interagire con lo stesso (ad esempio, valvole dell'aria condizionata che reagiscono alla presenza di persone).

mazioni in tempo reale sui consumi e consentire ai fornitori di energia elettrica di monitorare a distanza gli apparecchi elettrici; e, infine, ai vantaggi in termini di aumento dell'efficacia del ciclo produttivo derivanti da un più facile scambio di informazioni consentito dagli oggetti intelligenti in settori tradizionali quali la logistica, il settore manifatturiero e quello della distribuzione commerciale. Questi dispositivi utilizzano diverse tecnologie di base, quali la RFID (identificazione a radiofrequenza), la tecnologia NFC, i codici a barre 2D (codici a barre, Datamatrix), i sensori di comando senza fili, la versione 6 del protocollo Internet (Ipv6), la banda ultralarga o 3/4G, le nanotecnologie, in particolare quelle applicate ai microprocessori. Inutile dire che su queste tecnologie si tornerà più avanti, anche in ragione delle problematiche giuridiche che le stesse sollevano[47].

Occorre ora spendere qualche parola sulle procedure che portano alla fissazione degli standard della rete.

Il protocollo TCP/IP fu sviluppato dai ricercatori che diedero vita al progetto ARPAnet[48]. Da allora molte cose sono cambiate. Quello che viene considerato il nucleo originario di Internet si è accresciuto ospitando dapprima le sole organizzazioni a carattere scientifico, ma successivamente anche altri soggetti e, via via, chiunque, comprese le organizzazioni commerciali con scopo di lucro. I costi di gestione della rete vengono sopportati dai singoli network che si interconnettono ad essa.

Proprio in ragione della filosofia che la ispira, Internet non ha un vertice e non contempla autorità di governo centrale. Esistono alcuni organismi che lavorano costantemente al perfezionamento degli standard tecnici e alla manutenzione dei collegamenti. Tra questi organismi si possono ricordare:

1) Internet Society (ISOC). È un'organizzazione internazionale non governativa, su base volontaria (*not-for-profit corporation*) che si occupa della crescita e dell'evoluzione mondiale di Internet, delle modalità con le quali quest'ultima è o può essere usata, e dei problemi sociali, politici e tecnici che da detto uso possono derivare[49].

[47] Su «Internet degli oggetti» cfr. la comunicazione della Commissione al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, dal titolo «L'Internet degli oggetti – Un piano d'azione per l'Europa», Bruxelles, 18 giugno 2009, COM (2009) 278 def.; nonché il parere del Comitato economico e sociale europeo: «L'Internet degli oggetti» (2009/C 77/15).

[48] La creazione della famiglia di protocolli TCP/IP viene attribuita a Robert Kahn e Vinton G. Cerf.

[49] Maggiori informazioni all'indirizzo http://www.isoc.org. La missione di ISOC è «assicurare libero sviluppo, evoluzione ed utilizzo di Internet a beneficio di tutte le persone attraverso il mondo».

2) Internet Architecture Board (IAB). È un comitato consultivo tecnico dell'ISOC. Ha compiti di supervisione sull'architettura e sui protocolli di Internet[50].

3) Internet Engineering Steering Group (IESG). Fa parte dell'ISOC ed è responsabile dell'organizzazione tecnica dell'attività dell'IETF (cfr. punto 4) e del processo per la formazione degli standard di Internet. A questo organo spetta l'approvazione definitiva delle specifiche come standard di Internet[51].

4) Internet Engineering Task Force (IETF). Cura la definizione e lo sviluppo degli standard e dei protocolli di Internet[52]. È composto (su base volontaria, perché l'accesso è libero a chiunque) da progettisti di reti, operatori, venditori, ricercatori interessati all'evoluzione di Internet.

5) Internet Corporation for Assigned Names and Numbers (ICANN). È un organismo non profit che sovraintende all'allocazione degli indirizzi IP, all'assegnazione dei parametri dei protocolli, alla gestione degli indirizzi di dominio[53] [Pascuzzi 1999a] (sugli indirizzi IP e sui nomi di dominio cfr., nella seconda parte, le pagine dedicate a detti temi).

Protocolli, standard e specifiche di Internet sono contenuti in documenti denominati RFC (acronimo di *Request for comments*: è stato mantenuto il nome dei messaggi che gli architetti di ARPAnet si scambiavano tra loro per chiedere alla comunità come potevano essere risolti certi problemi)[54].

Tradizionalmente le attività di questi organismi esaurivano ciò che può essere definito «governo della rete» [Rossello 2006]. Con l'andare del tempo, però, si è reso necessario definire meglio la cosiddetta *Internet governance* anche per sottrarla al controllo di fatto dei paesi (Stati Uniti in testa) che hanno visto nascere la rete e renderla realmente espressione di un apporto planetario. Su questo tema si tornerà nella seconda parte del volume, nel capitolo dedicato alla destatualizzazione.

4. DIRITTO E INFORMATICA: UN RAPPORTO COMPLESSO

L'impatto delle tecnologie digitali sul mondo del diritto può essere paragonato ad una svolta epocale. Non c'è alcuna enfasi nel dire che l'in-

[50] Maggiori informazioni all'indirizzo http://www.iab.org.

[51] Maggiori informazioni all'indirizzo http://www.ietf.org/iesg.html.

[52] Maggiori informazioni all'indirizzo http://www.ietf.org.

[53] Maggiori informazioni all'indirizzo http://www.icann.org.

[54] Maggiori informazioni all'indirizzo http://www.rfc-editor.org.

formatica e la telematica attraversano in profondità il fenomeno giuridico provocando radicali trasformazioni nel modo di organizzare il pensiero, nel modo di lavorare, nel modo di educare. Prima di concentrarsi sull'obiettivo del presente lavoro conviene ricordare alcune di queste vicende.

4.1. Informatica e conoscenza

Negli ultimi anni tutti i saperi hanno fatto passi da gigante: c'è stato un accumulo enorme di conoscenze. Sono nati nuovi saperi. Sono cambiati i contenuti dei saperi.

L'informatica e la telematica stanno contribuendo in misura non secondaria a siffatta trasformazione.

a) La produzione della conoscenza

La società dell'informazione si caratterizza per un progressivo diffondersi di modelli di produzione innovativi rispetto a quelli tradizionali, denominati *Commons-based peer production* (produzione tra pari di beni di proprietà comune). Tra le forme di partecipazione condivisa alla costruzione di informazione e conoscenza, con le relative implicazioni attinenti agli strumenti di rete e all'adozione di formati di dati aperti, si possono citare Wikipedia[55], PlanetMath[56], Open Knowledge[57]. Questi sistemi di produzione e distribuzione di informazioni, opere digitali e quant'altro, traggono origine dall'applicazione dei principi di condivisione della conoscenza tipici del software libero (su cui cfr. il capitolo sul diritto d'autore), che rappresenta uno degli esempi più conosciuti e studiati di questo fenomeno [Rossato 2006][58].

[55] Cfr. http://www.wikipedia.org. Su Wikipedia, enciclopedia libera e multilingue, sviluppata in modo collaborativo su Internet, si tornerà nel capitolo dedicato al diritto d'autore.

[56] Cfr. http://www.planetmath.org.

[57] Cfr. http://wiki.okfn.org.

[58] Esiste anche un risvolto simpatico dell'ausilio che i computer possono dare alla produzione di conoscenza. È il caso di SCIgen, un programma che genera automaticamente *random*

b) La rappresentazione della conoscenza

L'esplosione dei saperi e la necessità di rendere sempre più efficace l'apprendimento danno vita a quello che può essere considerato uno dei problemi cruciali del nostro tempo: la rappresentazione della conoscenza. Sono sempre più frequenti le ipotesi in cui occorre essere in grado di conoscere in breve tempo un certo patrimonio di conoscenza (per verificare ipotesi, nel dialogo tra i saperi, per studiare un campo disciplinare diverso dal nostro, per fare propri i tratti salienti di un diverso sistema giuridico). Nel campo del diritto, la scrittura lineare costituisce lo strumento principale di rappresentazione della conoscenza. È anche il più efficace?

Per centinaia di anni la riflessione giuridica è stata rappresentata mercé l'utilizzo della scrittura lineare che costituisce il dato unificante dei generi letterari succedutisi nelle diverse epoche e nei diversi luoghi (monografie, enciclopedie, commentari, trattati, manuali, dizionari, rassegne, ecc.). L'ingresso sulla scena dell'informatica prima e della telematica poi ha comportato la nascita di generi letterari alternativi: forme espressive che traggono dal supporto elettronico la propria peculiarità e che consentono di ipotizzare nuovi metodi per produrre cultura e conoscenza.

L'esempio più rappresentativo dei generi letterari elettronici è rappresentato dall'ipertesto (anche perché ipertestuale è l'architettura del web, ossia il più diffuso sistema di navigazione in Internet). I giuristi (ma non solo loro) operano mettendo insieme, nel modo reputato migliore, un certo numero di elementi della conoscenza al fine di perseguire risultati quali la soluzione di un problema ovvero la produzione di nuova conoscenza. Gli elementi sono scelti e accostati in ragione di relazioni di tipo associativo in vista della costruzione di un percorso cognitivo che poi viene rappresentato in discorsi orali o scritti. L'ipertesto è molto affine al modo di procedere appena descritto. Esso è strutturalmente destinato ad evidenziare, anche visivamente, i meccanismi associativi e i segmenti in cui si snoda il ragionamento. Si tratta di caratteristiche innovative rispetto alle tecnologie della

paper scientifici in materia di *computer science*: http://pdos.csail.mit.edu/scigen. SCIgen assembla dal nulla anche grafici, tabelle e citazioni. Il programma è stato realizzato da tre giovani studiosi statunitensi con lo scopo di screditare le conferenze scientifiche con bassi standard qualitativi organizzate solo per fare soldi.

parola tradizionali. L'esposizione del ragionamento giuridico è anche un problema di costruzione del testo. In fondo i diversi generi letterari altro non sono che modalità più o meno alternative di costruzione del testo (e di organizzazione dei dati).

Così come il libro stampato (sinonimo di gerarchia, linearità, standardizzazione del testo e della sua collocazione sulla pagina) ha plasmato il modo di ragionare degli uomini [Eisenstein 1985; 1999; Febvre e Martin 1988; McLuhan 1991], ci si può aspettare una riorganizzazione del pensiero da generi letterari elettronici che ridisegnano il rapporto tra autore e lettore ridefinendo le trame narrative in funzione delle possibili elaborazioni della base informativa [Pascuzzi 1997].

c) L'accesso alla conoscenza

L'accumulo di conoscenze rende ancora più urgente il problema dell'accesso alle medesime. Nella società dell'informazione la tematica della fruizione del lavoro intellettuale è il discrimine intorno al quale si definisce il modello stesso di società. Il 4-5 novembre 2004, in occasione di un convegno promosso dalla CRUI (Conferenza dei rettori italiani) presso l'Università di Messina[59], numerose università hanno sottoscritto un documento[60] di sostegno alla *Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities*, secondo la quale il compito dei sottoscrittori, membri delle comunità scientifiche,

> is only half complete if the information is not made widely and readily available to society. New possibilities of knowledge dissemination not only through the classical form but also and increasingly through the open access paradigm via the Internet have to be supported.

Nella traiettoria indicata un ruolo significativo sta assumendo il progetto

[59] Cfr. gli atenei italiani per l'*open access*: verso l'accesso aperto alla letteratura di ricerca, http://www.aepic.it/conf/index.php?cf=1.

[60] Cfr. http://www.aepic.it/conf/viewpaper.php?id=49&cf=1.

Creative Commons [Lessig 2004; Ziccardi 2005, 31][61]. Nata come associazione senza fini di lucro nel 2001, con il supporto del Center for Public Domain e per ispirazione di giuristi quali Lessig e Boyle, l'iniziativa si prefigge di predisporre una serie di licenze che possano essere utilizzate nelle arti e nelle scienze per la diffusione di opere intellettuali, creando una forma di appartenenza collettiva, un *common* appunto, per le opere letterarie, musicali, audiovisive, ecc. Si segnalano tentativi volti ad applicare questi principi alle scienze biologiche e mediche. Nel 2005 è partito *Science Commons*, che si propone di incoraggiare l'innovazione scientifica, facilitando agli scienziati, alle università e alle industrie, l'uso di letteratura, dati e altri oggetti di proprietà intellettuale e la condivisione della loro conoscenza con gli altri. L'obiettivo è promuovere strumenti giuridici e tecnici volti a eliminare le barriere alla condivisione[62].

4.2. Informatica e organizzazione del lavoro

I mutamenti prodotti dalle nuove tecnologie coinvolgono anche il mondo del lavoro: alcune figure professionali stanno scomparendo mentre se ne creano di nuove. Informatica e telematica rendono le attività lavorative sempre più indipendenti dalla localizzazione fisica di strutture e risorse, favorendo una nuova forma di organizzazione del lavoro: il telelavoro [Lucafò 2007; Toffoletto 2006]. Essa permette di operare rimanendo distanti dal tradizionale posto di lavoro, nelle mura della propria casa, in un centro appositamente allestito, o in un qualsiasi posto (telelavoro mobile)[63]. Elementi che caratterizzano il telelavoro sono, infatti: la delocalizzazione produttiva; l'utilizzo intenso di sistemi informatici; l'esistenza di una rete di comunicazione (dell'impresa o infrastrutturale); la modifica della struttura organizzativa tradizionale; la flessibilità di erogazione, impiego e gestione del lavoro[64].

[61] Cfr. http://creativecommons.org; nonché http://www.creativecommons.it.

[62] Cfr. http://www.creativecommons.it/ScienceCommons.

[63] Per quel che attiene la disciplina normativa, cfr. l'art. 4, legge 16 giugno 1998, n. 191, e il d.p.r. 8 marzo 1999, n. 70.

[64] Sull'identificazione del luogo della prestazione e sulla possibilità di modificarlo cfr. Trib. Milano, 20 dicembre 2005, in «Orient. giur. lav.», 2006, I, 118 e Trib. Napoli, 13 febbraio 2003, in «Foro it.», 2004, I, c. 635.

Anche il mondo delle professioni legali è interessato da mutamenti significativi [Ziccardi 2005].

La figura del notaio è destinata ad assumere funzioni nuove, ad esempio, in ragione delle nuove esigenze connesse alle certezze dei traffici telematici [Bortoluzzi 2004].

L'attività degli avvocati deve misurarsi con innovazioni che vanno dalla possibilità di fornire consulenze *on-line* alla creazione di reti di professionisti [Pascuzzi 2002; Alpa 2000; Zeno Zencovich 2000]. Per altro verso, la potenza comunicativa delle pagine web alimenta l'annoso problema della possibilità per gli iscritti agli albi professionali di farsi pubblicità[65].

Avvocati e magistrati sono coinvolti dall'introduzione del c.d. processo civile telematico, cui è dedicato un paragrafo nel capitolo sul documento elettronico. E non è certo secondario il ruolo che l'informatica può avere ai fini della razionalizzazione degli uffici giudiziari[66].

4.3. Informatica e formazione del giurista

Il tema della formazione del giurista negli ultimi tempi è oggetto di rinnovato interesse anche alla luce delle numerose riforme degli ordinamenti didattici succedutesi nel nostro paese (cosiddetti «3+2» e «1+4»). Si tratta di un tema con molte articolazioni: la formazione di base del giurista; la

[65] L'art. 17-*bis*, ultimo comma, del codice deontologico degli avvocati, recita: «L'avvocato può utilizzare esclusivamente i siti web con domini propri e direttamente riconducibili a sé, allo studio legale associato o alla società di avvocati alla quale partecipa, previa comunicazione tempestiva al Consiglio dell'Ordine di appartenenza della forma e del contenuto in cui è espresso. Il professionista è responsabile del contenuto del sito e in esso deve indicare i dati previsti dal comma 1 (dell'art. 17-*bis*). Il sito non può contenere riferimenti commerciali e/o pubblicitari mediante l'indicazione diretta o tramite *banner* o *pop-up* di alcun tipo».

[66] Presso il ministero di Giustizia opera la Direzione generale per i sistemi informativi automatizzati che è competente, tra l'altro, per la programmazione, la progettazione, lo sviluppo e la gestione dei sistemi informativi automatizzati di tutti gli uffici del ministero, degli uffici amministrativi decentrati e degli uffici giudiziari; per l'integrazione e l'interconnessione dei sistemi informativi del ministero per l'interconnessione con i sistemi informativi automatizzati delle altre amministrazioni per il tramite della rete unitaria delle pubbliche amministrazioni (cfr. art. 6, d.p.r. 55/2001). Su quest'ultimo aspetto si rinvia al sito del Centro nazionale per l'informatica nella pubblica amministrazione: www.cnipa.gov.it ora DigitPA, www.digitpa.gov.it. L'informatizzazione degli uffici giudiziari è uno dei temi approfonditi dal Centro per l'organizzazione, il management e l'informatizzazione degli uffici giudiziari (COMIUG): www.comiug.it.

formazione del professionista (avvocato, magistrato, notaio); la formazione continua e permanente.

Occorre considerare, inoltre, che la riforma dell'istruzione superiore promossa dal c.d. «processo di Bologna» (www.bolognaprocess.it) e da alcuni provvedimenti dell'Unione europea (si vedano in particolare la raccomandazione del Parlamento europeo e del Consiglio del 18 dicembre 2006, relativa a competenze chiave per l'apprendimento permanente, e la raccomandazione del Parlamento europeo e del Consiglio del 23 aprile 2008 sulla Costituzione del Quadro europeo delle qualifiche per l'apprendimento permanente) impongono di costruire i percorsi didattici in funzione dei risultati dell'apprendimento intesi come somma non solo dei saperi disciplinari ma anche di abilità e competenze.

Ne deriva che la formazione del giurista deve propiziare (oltre che l'apprendimento del sapere giuridico anche) l'apprendimento di abilità e competenze. Il giurista non deve solo «sapere» ma deve anche «saper essere» giurista e «saper fare» il giurista. In un recente lavoro [Pascuzzi 2008a] è stato redatto un inventario delle abilità che il giurista deve padroneggiare insieme, ovviamente, al sapere disciplinare.

Nella formazione tradizionale l'accento è posto sulla trasmissione di conoscenze, molto meno sulla trasmissione di abilità; sul «cosa» insegnare e non sul «come».

Computer e telematica mettono a disposizione strumenti in grado di integrare i tradizionali modelli di insegnamento e di prefigurare canali di apprendimento del tutto innovativi [Pascuzzi 2003a; Lugoboni 2002][67].

La tecnologia può innanzitutto essere usata per rendere più efficace la lezione frontale del docente (modello che attualmente contraddistingue le facoltà di Giurisprudenza). A mo' di esempio di questo tipo di approccio possono essere citati: l'utilizzo delle presentazioni basate su lucidi elettronici (ad esempio Power Point); la disponibilità su Internet dei materiali relativi al corso; la produzione di *casebooks* e ipertesti elettronici [Pascuzzi

[67] La Commissione europea ha realizzato un portale dedicato all'uso delle tecnologie dell'informazione e della comunicazione per migliorare l'apprendimento: http://www.elearningeuropa.info.

2001a]; l'attivazione di forum via e-mail tra gli studenti del corso; la didattica assistita da calcolatore[68], ecc.

Ma la tecnologia permette di ipotizzare contesti educativi del tutto nuovi: si tratta, in particolare, di contesti che prescindono dalla necessaria compresenza nello stesso luogo e nello stesso tempo del professore e dello studente.

Nella c.d. *extended classroom*, la lezione tenuta dal docente può essere seguita da una pluralità di studenti in differenti località remote attraverso sistemi di telecomunicazione, ovvero in videoconferenza, ovvero in videoconferenza via web, ecc. A seconda dei casi, varia il livello di interazione tra docenti e studenti in remoto.

Lo scenario sicuramente più innovativo è però rappresentato dal *classroom-free learning* (università *on-line*). Interi corsi universitari (composti di materiali, registrazioni audio e video, letture, *tutorial* di autoapprendimento e autoverifica) possono essere seguiti dagli studenti tramite Internet. Gli studenti hanno la possibilità di seguire i corsi senza essere vincolati da orari e da luoghi prefissati, modellando l'impegno cognitivo in ragione delle proprie disponibilità di tempo. Non sono certamente pochi gli esempi di università prestigiose (ma anche di soggetti privati che si stanno all'uopo attrezzando) che impartiscono corsi (e titoli di studio) interamente *on-line*.

Con decreto del 17 aprile 2003 (GU n. 98 del 29 aprile 2003) il ministro dell'Istruzione, Università e Ricerca di concerto con il ministro per l'Innovazione e la Tecnologia ha definito i criteri e le procedure per l'accreditamento dei corsi universitari a distanza e delle istituzioni universitarie abilitate al rilascio di titoli accademici di cui all'art. 3, d.m. 3 novembre 1999, n. 509[69]. Sulla

[68] Il CALI (Center for Computer-assisted Legal Instruction) è un consorzio di università statunitensi specializzato nella produzione di *tutorials*, esercizi, simulazioni, volti a favorire l'apprendimento del diritto (http://www.cali.org). Di qua dall'Atlantico operano con finalità simili il Computer-assisted Learning (CAL) e il Group of BILETA (British and Irish Legal Education Technology Association, http://www.bileta.ac.uk).

[69] A norma di detto decreto (art. 3), i corsi di studio a distanza sono caratterizzati da: *a*) l'utilizzo della connessione in rete per la fruizione dei materiali didattici e lo sviluppo di attività formative basate sull'interattività con i docenti/tutor e con gli altri studenti; *b*) l'impiego del personal computer, eventualmente integrato da altre interfacce e dispositivi, come strumento principale per la partecipazione al percorso di apprendimento; *c*) un alto grado di indipendenza del percorso didattico da vincoli di presenza fisica o di orario specifico; *d*) l'utilizzo di contenuti didattici standard, interoperabili e modularmente organizzati, personalizzabili rispetto alle caratteristiche degli utenti finali e ai percorsi di erogazione; *e*) il monitoraggio continuo del livello di apprendimento, sia attraverso il tracciamento del percorso che attraverso frequenti momenti di valutazione e autovalutazione. L'organizzazione didattica dei corsi di studio a distanza, inoltre, deve valorizzare al massimo, pur nel rispetto delle specificità dei contenuti e degli obiettivi didattici, le potenzialità dell'*Information & communication technology* e in particolare: *a*) la multimedialità, valorizzando un'effettiva integrazione tra diversi media per favorire una migliore comprensione dei contenuti; *b*) l'interattività con i materiali, allo scopo di favorire percorsi di studio personalizzati e di ottimizzare l'apprendimento; *c*) l'interattività umana, con la valorizzazione di tutte le tecnologie di comunicazione in rete, al fine di favorire la creazione di contesti collettivi di apprendimento; *d*) l'adattività, ovvero la possibilità di personalizzare la sequenzializzazione dei percorsi didattici sulla base delle performance e delle interazioni dell'utente con i contenuti *on-line*; *e*) l'interoperabilità dei sottosistemi, per il riutilizzo e l'integrazione delle risorse, utilizzati e/o generati durante l'utilizzo dei sistemi tecnologici.

base di detto decreto, alcune università telematiche hanno visto la luce nel nostro paese[70].

La rivoluzione digitale ha propiziato la nascita dell'*e-learning*. A ben vedere, però, l'*e-learning*, oggi più utilizzato, si fonda sulla parola e sul linguaggio per trasmettere e far acquisire conoscenza. Occorre pensare sempre più ad una «seconda stagione» dell'*e-learning* che batta strade diverse e innovative: l'utilizzo delle tecnologie informatiche per favorire l'apprendimento attraverso canali diversi dal linguaggio [Pascuzzi 2008b]. In particolare occorrerebbe sperimentare in che modo le simulazioni informatiche e la realtà virtuale possono facilitare l'apprendimento delle abilità.

Alcune esperienze già esistono. Nel cd-rom (acronimo di *Compact disk-read only memory*) di Pascuzzi, Bona e Roberti [2010], le simulazioni virtuali vengono usate per illustrare la disciplina sui rapporti di vicinato. Nel cd-rom allegato a Pascuzzi [2005a] è stato ricostruito un ambiente virtuale con il fine di far apprendere le abilità che è necessario padroneggiare per reperire i dati giuridici.

Occorre studiare in che modo le tecnologie informatiche possono favorire l'apprendimento delle abilità generiche e specifiche delle singole figure professionali ad esempio attraverso le simulazioni virtuali e i giochi di ruolo [Pascuzzi 2008c].

[70] La produzione di contenuti per la didattica *on-line* può essere ostacolata quando vengono utilizzati materiali (articoli di dottrina, parti di manuali, fotografie, opere audiovisive, brani musicali e così via) coperti da diritti d'autore. Per adoperare e diffondere tali contenuti è necessario ottenere il consenso dei soggetti che su di essi vantano i diritti morali e patrimoniali di paternità e sfruttamento economico. Oppure è necessario avvalersi delle eccezioni al diritto d'autore previsti nelle legislazioni nazionali e sovranazionali entro i limiti dalle stesse individuati [Vezzoso 2009]. Si veda, ad esempio, l'art. 5, par. 3, lett. *a*, e par. 5, della direttiva 2001/29/CE; il d.lgs. 68/2003; gli artt. 68 ss., legge 633/1941 sul diritto d'autore.

Va da sé che quanto offerto (nello specifico ambito in esame) dalla tecnologia non è necessariamente di segno positivo e come tale destinato a soppiantare i paradigmi educativi esistenti. Taluni si mostrano scettici circa la reale possibilità che gli strumenti appena descritti sostituiscano oltre una certa soglia la tradizionale lezione cattedratica. Questi autori, tuttavia, sottolineano come l'insegnamento a distanza possa giocare un ruolo decisivo in contesti specifici, come ad esempio la formazione continua degli avvocati[71].

Resta il fatto che sarebbe erroneo non scandagliare le potenzialità che vengono offerte e soprattutto verificare in che modo le tecnologie digitali possano assicurare la trasmissione delle abilità che sempre più devono entrare a far parte del bagaglio formativo del giurista.

4.4. Informatica e diffusione dei materiali giuridici (normativa, decisioni giurisprudenziali, dottrina)

Nell'impostazione tradizionale gli atti normativi, le pronunce giurisprudenziali e i contributi dottrinali vengono conservati e diffusi su supporti cartacei: libri, riviste, repertori di giurisprudenza, raccolte di leggi, ecc. L'avvento dei calcolatori sta rivoluzionando questo scenario. Oltre che tramite le edizioni cartacee, è oggi possibile consultare i materiali giuridici servendosi

[71] Il 13 luglio 2007 il Consiglio nazionale forense ha approvato il regolamento sulla formazione continua che impone agli avvocati iscritti all'albo di mantenere e aggiornare la propria preparazione professionale partecipando alle attività di formazione professionale continua. Con tale espressione si intende ogni attività di accrescimento ed approfondimento delle conoscenze e delle competenze professionali, nonché il loro aggiornamento mediante la partecipazione ad iniziative culturali in campo giuridico e forense. Anche il Consiglio nazionale del notariato, rifacendosi all'art. 2 del codice deontologico dei notai che impone a detti professionisti di «curare l'aggiornamento della propria preparazione professionale mediante l'acquisizione di specifiche conoscenze in tutte le materie», ha emanato un regolamento volto ad introdurre l'obbligo della formazione permanente a partire dal 1° gennaio 2006. Si moltiplicano sulla rete gli esempi di corsi di aggiornamento impartiti *on-line*. Sul sito del CNF, ad esempio, si può seguire un corso di formazione per difensori d'ufficio (http://www.consiglionazionaleforense.it/on-line/Home/Formazione/E-learning/artCatCorsi.2037.1.5.1.1.html). Nel settore si stanno muovendo anche operatori privati: per l'IPSOA cfr. il sito http://shop.wki.it/linea.aspx?linea=elearning&idlinea=2006. Per ora, pur essendo le tecnologie mature, la tendenza è a proporre video registrati e a somministrare materiali digitalizzati. Sembra ancora lontana, almeno in ambito giuridico, una riflessione tesa a formulare i contenuti sulla base delle potenzialità del mezzo: un video non è affatto sinonimo di interattività. Resta in ogni caso il problema della certificazione delle attività svolte *on-line*. Per alcune esperienze straniere si consultino i seguenti siti: http://clecenter.com; http://www.objection.com.

dei computer grazie alle edizioni su cd-rom e alle banche dati *on-line* [Pascuzzi 2003a; Bin e Lucchi 2009].

All'informatica i giuristi hanno chiesto innanzitutto di fornire strumenti utili a governare e reperire in modo più agevole i materiali normativi, giurisprudenziali e dottrinali. Gli albori della storia dei generi letterari elettronici coincidono con la «documentaristica informatizzata». Le banche dati *on-line* hanno rappresentato la prima risposta a quel tipo di sollecitazione[72]. Si è così fatto strada un nuovo modello di conservazione e trasmissione del patrimonio conoscitivo giuridico le cui peculiarità possono essere così sintetizzate:

1) modalità innovative di archiviazione e fruizione dell'informazione. Il metodo tradizionale di diffusione delle informazioni impone al fruitore di raggiungere il luogo fisico in cui l'informazione è conservata (ad esempio una biblioteca), ovvero di procurarsi il singolo volume. Siffatto scenario muta in ragione della possibilità, inerente al dato elettronico, di «viaggiare» su reti telematiche: il dato viene immagazzinato in un unico posto (l'elaboratore centrale) e può essere consultato da qualsivoglia punto del globo;

2) più puntuale e rapido reperimento dei dati. I software di *information retrieval* passano in rassegna, in frazioni di secondo, tutti i documenti immagazzinati al fine di trovare quelli che rispondono alle condizioni imposte dall'utilizzatore nella stringa di ricerca[73];

3) continuo aggiornamento dei dati. L'accentramento in un luogo della conservazione delle informazioni rende più facile la fruizione immediata dei

[72] Banca dati può essere definito ogni insieme di informazioni su un argomento particolare in forma elettronica. A volte le banche dati contengono il documento integrale (c.d. informazioni fattuali). Ad esempio le banche dati *full-text* come *Lexis*. Altre volte forniscono solo riferimenti ai documenti originali (come libri, articoli), indicando autore, collocazione, ecc. Ad esempio gli schedari bibliografici delle biblioteche. Per quest'ultima tipologia, alcuni usano il termine «base dati» per distinguerla dalla prima. L'attributo *on-line* individua un sistema di ricerca delle informazioni che permette di effettuare direttamente la ricerca in modo interattivo da un terminale a distanza.

[73] L'interrogazione di una banca dati mira a reperire documenti che rispondano alle condizioni imposte nella stringa di ricerca. Tra le condizioni può esserci, ad esempio, quella per cui nel documento appaiano determinate parole. Orbene, tramite gli operatori logici booleani è possibile combinare le condizioni (nel nostro caso: le parole) al fine di meglio perseguire l'obiettivo di reperire solo i documenti desiderati e non altri. Per definire in maniera puntuale l'ambito della ricerca si possono cercare documenti ove compaiono contestualmente più parole (ad esempio «vendita» e «proprietà»), ovvero compaiano alcune parole e non altre (ad esempio «interessi» ma non «legittimi») o, ancora, siano presenti alternativamente più parole (ad esempio «riservatezza» oppure «privacy») [Sartor 2008; Taddei Elmi 2006].

mutamenti sopravvenuti: le banche dati *on-line* vengono di regola aggiornate nottetempo con le modifiche o gli arricchimenti di informazioni eventualmente intervenuti, affinché tutti gli utilizzatori possano avvantaggiarsene in tempo reale.

Il vero punto di forza delle edizioni in parola sta nell'enorme mole di documentazione messa a disposizione tanto dei pratici quanto dei ricercatori, che vedono schiudersi scenari inimmaginabili nel regno dominato dalla carta.

Dopo le prime esperienze pionieristiche, oggi sono moltissime le banche dati giuridiche sparse un po' ovunque nel mondo.

PARTE PRIMA

Come le tecnologie digitali cambiano le regole giuridiche

CAPITOLO 1

Dal diritto alla riservatezza alla computer privacy

Il diritto è plasmato dalle tecnologie disponibili, con la conseguenza che esso è destinato a cambiare in ragione dell'avvento di nuove tecnologie.

L'affermazione secondo la quale le regole giuridiche sono legate a filo doppio alle tecnologie che ne hanno propiziato e favorito la creazione può assumere significati diversi.

Il cambio di tecnologia può, innanzitutto, comportare il mutamento del contenuto di una determinata posizione giuridica tutelata e una modifica degli approcci con i quali si persegue la tutela. È quanto si cercherà di dimostrare in questo capitolo dedicato al diritto alla *computer privacy*.

La storia del diritto alla riservatezza copre un arco temporale di poco superiore al secolo. Di *Right to privacy* si comincia a parlare esplicitamente, oltre Atlantico, alla fine dell'800, in un articolo apparso sulla «Harvard Law Review» a firma di Warren e Brandeis [1890][1]. Nel vecchio continente, ai primi del '900 si intraprende (per mano soprattutto dei giuristi tedeschi) la costruzione della categoria dei «diritti della personalità» [Zeno Zencovich 1995; Resta 2005][2].

[1] Il tema fu affrontato incidentalmente, nell'ambito di un trattato sui fatti illeciti, dal giudice Thomas Cooley [1888]. Nel testo la privacy viene definita come *right to be let alone*. Nella *dissenting opinion* del caso *Olmstead vs. United States*, 277 U.S. 438 (1928), *Justice* Brandeis scriveva: «The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. [...] They conferred, as against the Government, the right to be let alone – the most comprehensive of rights, and the right most valued by civilized men».

[2] L'art. 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (firmata a Roma il 4 novembre 1950) riconosce ad ogni persona il diritto al rispetto della sua vita

In Italia, il problema dell'esistenza di un diritto alla riservatezza si è affacciato nel secondo dopoguerra in relazione alla divulgazione (ad opera di mezzi di comunicazione di massa o in trame cinematografiche) di fatti inerenti la sfera intima di persone famose. A metà degli anni '50 la Cassazione negò l'esistenza nel nostro sistema del diritto alla riservatezza (Cass., 22 dicembre 1956, n. 4487)[3]. La questione era sorta in merito alla realizzazione di due film riguardanti la vita del celebre tenore Enrico Caruso[4]. Le pellicole rappresentavano, in modo romanzato, fatti della vita privata dell'artista che i familiari consideravano lesivi della sua riservatezza. Si trattava di passaggi filmati, ritenuti non veritieri, nei quali, a detta degli eredi, la figura del grande tenore risultava danneggiata. In particolare vi erano sequenze che descrivevano l'umile ambiente nel quale il tenore era vissuto in giovinezza, la sua dedizione all'alcool che lo portava spesso all'ubriachezza, i conflitti con gli esattori delle imposte, gli alterchi con i colleghi, il tentativo di suicidio[5].

A metà degli anni '60 si comincia a intravedere un mutamento di rotta nell'orientamento della Corte suprema (Cass., 20 aprile 1963, n. 990)[6]. Il caso riguardava la pubblicazione di un libro nel quale l'autore ricostruiva alcuni aspetti della personalità di Claretta Petacci, l'amante di Mussolini. I familiari della donna citarono in giudizio l'autore e l'editore della pubblicazione perché, a loro dire, questa conteneva affermazioni e aspetti privati che violavano la riservatezza della Petacci offendendone la reputazione.

Nel 1975, dopo aver negato per molto tempo l'ammissibilità di una pro-

privata e familiare, del suo domicilio e della sua corrispondenza. Si veda anche l'art. 12 della Dichiarazione universale dei diritti dell'uomo del 10 dicembre 1949 nonché gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata a Strasburgo il 12 dicembre 2007, di cui all'art. 6 del Trattato dell'UE.

[3] La sentenza è riportata in «Foro it.», 1957, I, c. 4 con la seguente massima: «Nell'ordinamento giuridico italiano non esiste un diritto alla riservatezza, ma soltanto sono riconosciuti e tutelati, in modi diversi, singoli diritti soggettivi della persona; pertanto non è vietato comunicare, sia privatamente sia pubblicamente, vicende, tanto più se immaginarie, della vita altrui, quando la conoscenza non ne sia stata ottenuta con mezzi di per sé illeciti o che impongano l'obbligo del segreto».

[4] Uno intitolato *Il grande Caruso*, l'altro *Enrico Caruso: leggenda di una voce*.

[5] Giudicando lesa la riservatezza e l'onore del proprio familiare, gli eredi convennero in giudizio la società produttrice dei film.

[6] La sentenza è riportata in «Giust. civ.», 1963, I, p. 1280 con la seguente massima: «Sebbene non sia ammissibile il diritto tipico alla riservatezza, viola il diritto assoluto di personalità, inteso quale diritto *erga omnes* alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo, la divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito ed ove non sussista per la natura dell'attività svolta dalla persona e del fatto divulgato un preminente interesse pubblico di conoscenza».

tezione autonoma del rispetto della vita privata, il Supremo Collegio, conformandosi ad una copiosa giurisprudenza di merito[7], perviene all'affermazione che l'ordinamento giuridico riconosce e tutela l'interesse di ciascuno a che non siano resi noti fatti o avvenimenti di carattere riservato senza il proprio consenso. La sentenza affermava costituire lesione della privacy la divulgazione di immagini o avvenimenti non direttamente rilevanti per l'opinione pubblica, anche quando tale divulgazione venga effettuata con mezzi leciti e per fini non esclusivamente speculativi. La pronuncia veniva resa in una delle controversie instaurate da Soraya Esfandiari contro alcuni giornali che avevano pubblicato fotografie ritraenti l'ex imperatrice in atteggiamenti intimi con un uomo, nelle mura della propria abitazione (Cass., 27 maggio 1975, n. 2129)[8].

Il principio è stato successivamente più volte ribadito dalla corte di legittimità[9]. Quanto al fondamento normativo della tutela della riservatezza, esso è stato rinvenuto nelle numerose norme da cui emerge la volontà del legislatore di garantire il riserbo personale e familiare[10]. Dal canto suo la

[7] Pret. Roma, 19 novembre 1951, in «Foro it.», 1952; Trib. Roma, 14 settembre 1953, in «Giur. it.», 1954, I, 2, c. 532; App. Milano, 21 gennaio 1955, in «Foro it.», 1955, I, c. 386; App. Napoli, 20 agosto 1958, in «Giust. civ.», 1959, p. 1811; App. Milano, 26 agosto 1960, in «Foro it.», 1955, I, c. 386; App. Milano, 19 gennaio 1971, in «Foro it.», 1971, II, c. 24; Pret. Milano, 12 maggio 1972, in «Foro it.», 1972, I, c. 2706.

[8] La sentenza è riportata in «Foro it.», 1976, I, c. 2895 con la seguente massima: «Il nostro ordinamento riconosce il diritto alla riservatezza, che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificati da interessi pubblici preminenti».

[9] Cass., 5 aprile 1978, n. 1557; 13 marzo 1985, n. 1968; 7 febbraio 1996, n. 982; 7 febbraio 1996, n. 978; 16 gennaio 1991, n. 4031; 21 febbraio 1994, n. 1652.

[10] Cass., 9 giugno 1998, n. 5658 così ricorda tali norme: art. 614 c.p. (violazione di domicilio); 615-*bis* c.p. (interferenze illecite nella vita privata); art. 616 c.p. (segretezza della corrispondenza); legge 8 aprile 1974, n. 98 (riservatezza e libertà delle comunicazioni); art. 472, comma 2, c.p.p. (tutela della riservatezza dei testimoni e delle parti private in ordine a fatti che non costituiscono oggetto dell'imputazione); art. 19, r.d.l. 27 maggio 1929, n. 1285 (notizie raccolte in sede di rilevazioni statistiche); artt. 140 e 185, r.d.l. 9 luglio 1939, n. 1238 (registri dello stato civile, in particolare riservatezza circa la paternità o la maternità: leggi 586/1950 e 1064/1955); art. 93, legge 633/1941 (divieto di pubblicare corrispondenze o memorie che abbiano carattere confidenziale o si riferiscono all'intimità della vita privata); legge 300/1970 (divieto di indagini personali sul corpo e sulle opinioni del lavoratore); art. 24, legge 241/1990 e art. 8, d.p.r. 352/1992 (diritto di accesso ai documenti amministrativi e diritto alla riservatezza). Ci si ferma volutamente alla situazione anteriore alla legge 31 dicembre 1996, n. 675 (in tema di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali) su cui *infra*. È stato rilevato, inoltre, che il legislatore ordinario prende in speciale considerazione determinate manifestazioni personali, per apprestare specifici strumenti di tutela contro l'invadenza di altri interessi: così in ordine al corpo (art. 5 c.c.), al nome (artt. 6-9 c.c.), all'immagine (art. 10 c.c.), all'anonimato e all'inedito (artt. 21 e 24 legge sul diritto d'autore). Detta

dottrina ancorava nella Costituzione il fondamento normativo del diritto alla riservatezza, in particolare nell'art. 2 e nel riconoscimento dei diritti inviolabili della persona.

In sintesi: in un clima culturale propizio (nel 1970 in Francia era stato novellato l'art. 9 del codice civile per riconoscere esplicitamente il *droit à la vie privée*), al termine di un tormentato *iter* giurisprudenziale e sulla scorta delle opinioni dottrinali che ancoravano direttamente nella Carta fondamentale la tutela dell'interesse in parola, a metà degli anni '70 il diritto alla riservatezza trova pieno riconoscimento nel nostro ordinamento. In quel momento il contenuto del diritto alla riservatezza corrispondeva al diritto a essere lasciati soli[11].

1. DAL DIRITTO AD ESSERE LASCIATI SOLI AL DIRITTO AL CONTROLLO SULLE INFORMAZIONI CHE RIGUARDANO L'INDIVIDUO

Il momento che vede la definitiva affermazione nel nostro ordinamento del diritto alla riservatezza coincide con l'inizio della capillare diffusione dei calcolatori [Rodotà 1973; Alpa e Bessone 1984].

L'evoluzione recente dell'informatica può dividersi in quattro periodi. Il primo, che copre gli anni '70 del '900, è caratterizzato dalla presenza di pochi voluminosi calcolatori. Dato il costo elevato, sono le pubbliche amministrazioni gli unici soggetti che possono permettersi l'utilizzo di queste macchine. La minaccia è rappresentata dal possibile controllo governativo, con i conseguenti rischi di discriminazione legati alla raccolta

linea tendenziale del nostro ordinamento trova corrispondenza in diverse deliberazioni di carattere internazionale sottoscritte dall'Italia, quale la Dichiarazione universale sui diritti dell'uomo, approvata il 10 dicembre 1948 dall'ONU, da cui risulta vietata qualsiasi interferenza arbitraria nella vita privata dell'individuo, e la Convenzione europea, firmata a Roma il 4 novembre 1950 (resa esecutiva con legge 4 agosto 1955, n. 848) che all'art. 8 riconosce ad ogni persona il diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza.

[11] Cfr. Cass., sez. II, 21 febbraio 1994, n. 1652: «Seguendo una giurisprudenza ed una dottrina consolidate si riconosce la sussistenza di un diritto alla riservatezza; quest'ultima viene intesa come riserbo della intimità della vita domestica privata, di situazioni e vicende personali e familiari che si svolgono nell'ambito del proprio domicilio e che vanno tutelate da ingerenze di terzi, non giustificate da interessi generali e pubblici di carattere preminente».

di dati (c.d. sensibili) quali le origini razziali, le opinioni politiche e sindacali, ecc.

Il secondo periodo attraversa gli anni '80. I computer costano meno e diventano poco ingombranti. Possono essere utilizzati anche da grandi imprese private (banche, assicurazioni, ecc.).

Il terzo periodo copre la prima metà degli anni '90 e si può dire concluso con l'emanazione della legge sul trattamento dei dati personali (675/1996) [Pardolesi 2003], oggi confluita nel codice in materia di protezione dei dati personali (d.lgs. 196/2003). I computer costano sempre meno e ormai sono presenti in tutte le case, così che chiunque può agevolmente raccogliere informazioni sugli individui.

Il quarto periodo, corrispondente all'ultimo decennio, coincide con l'utilizzo di massa delle reti telematiche: Internet entra a far parte del nostro agire quotidiano, dando la stura a problemi di non poco momento, attesa la difficoltà di dare effettività alla tutela in un contesto per definizione aterritoriale.

Nel torno di anni appena individuato si è assistito ad un proliferare di normative emanate (anche a livello sovranazionale) con l'intento di disciplinare il trattamento dei dati personali mercé l'utilizzo di calcolatori elettronici. Tali normative (spesso anche novellate) risentono dell'evolversi della rivoluzione digitale così come sopra delineata.

L'Italia ha anticipato solo la Grecia, tra i paesi occidentali, nel dotarsi di una normativa in materia, ma conviene ricordare che le prime leggi svedesi e tedesche risalgono agli inizi degli anni '70. La legge francese è del 1978.

A livello sovranazionale va ricordata la copiosa produzione di raccomandazioni emanata in materia dal Consiglio d'Europa che si è fatto promotore anche della Convenzione per la protezione degli individui con riguardo al trattamento automatizzato di dati personali (Strasburgo, 28 gennaio 1981), ratificata in Italia con legge 21 febbraio 1989, n. 98.

Anche l'Unione europea è intervenuta nel settore con la direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla «tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati»; con la direttiva 97/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997 sul «trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomu-

nicazioni»[12], poi abrogata e sostituita dalla direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al «trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)»[13], a propria volta recentemente emendata dalla direttiva 2009/136/CE.

Naturalmente non è possibile in questa sede analizzare dettagliatamente siffatte normative. Ai fini del presente lavoro è sufficiente notare che le normative sul trattamento computerizzato dei dati personali perseguono tutte un obiettivo finale: assicurare all'interessato il controllo sul flusso delle informazioni che lo riguardano.

Scrive Stefano Rodotà [1999, 201, corsivi aggiunti]:

> Le discussioni teoriche e le complesse esperienze di questi anni mostrano che la privacy si presenta ormai come nozione fortemente dinamica e che si è stabilita una stretta e costante interrelazione fra mutamenti determinati dalle tecnologie dell'informazione (ma anche dalle tecnologie della riproduzione, dall'ingegneria genetica) e mutamenti dello stesso concetto. Una *definizione della privacy come «diritto ad essere lasciato solo»*, come semplice *riservatezza*, ha da tempo perduto significato generale, anche se individua un valore, continua a cogliere un aspetto essenziale del problema e può essere applicata a specifiche situazioni. Nella società dell'informazione tendono a prevalere definizioni funzionali della privacy che, in molti modi, fanno riferimento alla possibilità di un soggetto di conoscere, controllare, indirizzare, interrompere il flusso delle informazioni che lo riguardano. La privacy, quindi, può in primo luogo, e più precisamente, essere definita come *il diritto di mantenere il controllo sulle proprie informazioni*.

L'introduzione delle tecnologie informatiche ha comportato un cambiamento di non poco momento nel campo della tutela dei diritti della personalità. L'avvento dei calcolatori ha richiesto l'adozione di specifici meccanismi di tutela perché il problema non era più (solo) quello di salvaguardare la vita privata di persone famose dall'aggressione portata dai mass media, bensì quello di scongiurare i pericoli più o meno palesi e avvertibili (discriminazioni in testa) derivanti a ciascun cittadino dalla facilità con la quale possono essere trattate e incrociate informazioni che lo riguardano. La rivoluzione digitale comporta addirittura il cambiamento della nozione e del contenuto del diritto alla riservatezza: non più diritto ad essere lasciati soli, ma diritto al controllo sui propri dati.

[12] Si veda anche il regolamento CE 45/2001 del Parlamento europeo e del Consiglio del 18 dicembre 2000 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati.

[13] L'attuazione in Italia della produzione comunitaria si è compiuta con il d.lgs. 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali).

2. IL CODICE DELLA PRIVACY: IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

Nel nostro paese la disciplina relativa alla protezione dei dati personali è oggi contenuta nel d.lgs. 30 giugno 2003, n. 196, denominato «codice in materia di protezione dei dati personali» [Bianca e Busnelli 2007; Sica e Stanzione 2004; Rodotà 2004b; Monducci e Sartor 2004; Cardarelli, Sica e Zeno Zencovich 2004]. Il codice rappresenta forse il primo tentativo al mondo di ricondurre ad unità le innumerevoli disposizioni in materia di privacy: esso, infatti, riunisce in unico articolato la legge 675/1996 e gli altri decreti legislativi, regolamenti e codici deontologici che si sono succeduti in questi anni[14]. Introduce, inoltre, alcune importanti innovazioni facendo tesoro dei principi sanciti dall'Autorità garante (su cui *infra*) e dalla direttiva UE sulla riservatezza nelle comunicazioni elettroniche.

Conviene, sotto questo profilo, ricordare sin da subito il nuovo tassello che la produzione normativa più recente ha aggiunto al quadro concettuale inerente i diritti della personalità. È un'innovazione che per un verso integra, una volta di più, la nozione di riservatezza e, per altro verso, canonizza un autonomo diritto. L'art. 1, d.lgs. 196/2003 (d'ora in avanti: codice della

[14] L'art. 1, legge 24 marzo 2001, n. 127, aveva delegato al governo l'emanazione di un testo unico in materia di trattamento dei dati personali al fine di coordinare le norme al momento vigenti e apportare alle stesse le integrazioni e le modifiche necessarie al predetto coordinamento o per assicurare la migliore attuazione.

privacy), infatti, riconosce a ciascuno il «diritto alla protezione dei dati personali»[15]. L'autonomia di tale nuova posizione soggettiva appare avvalorata dal successivo art. 2, comma 1, del codice in parola, ove il diritto alla protezione dei dati personali viene normativamente riconosciuto e garantito accanto (e in aggiunta) al diritto alla riservatezza e a quello all'identità personale[16].

Il codice è diviso in tre parti: la prima contiene le disposizioni generali che riguardano tutti gli adempimenti e i corrispondenti diritti relativi al trattamento con riferimento ai settori pubblico e privato (in particolare contiene norme: sui principi generali, sui diritti dell'interessato, sulle regole generali per il trattamento dei dati, sui soggetti che effettuano il trattamento, sulla sicurezza dei dati e dei sistemi, sugli adempimenti e sul trasferimento dei dati all'estero); la seconda è la parte speciale dedicata a specifici settori (trattamenti in ambito giudiziario; da parte di forze di polizia; in ambito pubblico; in ambito sanitario; per scopi storici, statistici o scientifici; per scopi statistici o scientifici; nonché materie come: minori; difesa e sicurezza dello Stato; istruzione; lavoro e previdenza sociale; sistema bancario, finanziario ed assicurativo; comunicazioni elettroniche; libere professioni e investigazione privata; giornalismo ed espressione letteraria e artistica; marketing diretto); la terza parte del codice contiene le tutele amministrative e giurisdizionali, disciplina le sanzioni amministrative e penali e regolamenta l'Ufficio del Garante.

L'ambito di applicazione si estende al trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato. Comprende anche il trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un paese non appartenente all'Unione europea e impiega,

[15] La legge 15/2009 (art. 4, comma 9) ha introdotto un inciso nell'art. 1 del codice per statuire che le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto ad una funzione pubblica e la relativa valutazione non sono oggetto di protezione della riservatezza personale.

[16] In dottrina si attribuisce a tale distinto riconoscimento normativo il senso di tutelare autonomamente la libertà positiva dell'interessato a esercitare un controllo sulle vicende circolatorie delle informazioni che lo riguardano. Per una specificazione applicativa di questo modo di intendere il diritto alla protezione dei dati personali, con riferimento alla possibilità di azionare la tutela risarcitoria, ove il titolare distrugga dati personali, compromettendo sul piano probatorio le *chanches* dell'interessato di tutelare in giudizio un proprio diritto fondamentale [cfr. Izzo 2004, 160].

per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del codice della privacy solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli artt. 15 e 31 (cfr. art. 5 del codice)[17].

Il codice (art. 4) definisce i termini utilizzati nell'articolato. A cominciare dalla nozione di trattamento che ricomprende ogni accezione del ciclo di vita di una informazione. In particolare, la lett. *a* del comma 1 dell'articolo appena citato considera «trattamento» moltissime operazioni raggruppabili in quattro fasi che caratterizzano il ciclo di vita del dato: 1) la fase preliminare, in cui rientrano la raccolta e la registrazione; 2) la fase dell'utilizzo dei dati, in cui rientrano: l'organizzazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto e l'interconnessione; 3) la fase di circolazione dei dati, in cui rientrano la comunicazione[18] e la diffusione[19]; 4) la fase terminale, in cui rientrano la conservazione, il blocco[20], la cancellazione e la distruzione delle informazioni stesse.

La definizione di «dato personale» svolge, ovviamente, un ruolo significativo. Il codice specifica che tale espressione comprende qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione,

[17] Non si ha trattamento illecito di dati personali (*ex* art. 167, d.lgs. 196/2003) se esso avviene per fini esclusivamente personali, senza una loro diffusione o destinazione ad una comunicazione sistematica: Cass., 22 ottobre 2008, in «Ced Cass.», rv. 241966. Secondo Cass., 17 novembre 2004, in «Foro it.», 2006, II, c. 46, è penalmente lecita anche la comunicazione ad alcuni *providers*, senza consenso dell'interessato, di dati reperibili in pubblici registri, pubblici elenchi e siti Internet.

[18] Per «comunicazione» si intende il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

[19] Per «diffusione» si intende il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. In argomento cfr. Cass., sez. III pen., 9 giugno 2006, in «Giust. pen.», 2007, II, 282, secondo la quale non costituisce diffusione l'utilizzazione dei dati anagrafici e fiscali di un soggetto ai fini dell'intestazione di una scheda telefonica, poi consegnata in uso ad una terza persona.

[20] Per «blocco» si intende la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (cfr. art. 4, comma 1, lett. *b*)[21]. Una particolare categoria di dati, per i quali è dettata una disciplina specifica (cfr., ad esempio, artt. 20, 22, 23 e 26 del codice), è rappresentata dai cosiddetti «dati sensibili», di quei dati, cioè, particolarmente delicati in relazione alle forme di discriminazione più preoccupanti perché idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (cfr. art. 4, comma 1, lett. *d*)[22]. Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, costituisce una «banca di dati» (cfr. art. 4, comma 1, lett. *p*). È considerato «anonimo» il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile (cfr. art. 4, comma 1, lett. *n*).

Per quel che riguarda i soggetti coinvolti, il codice definisce «interessato» la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali (cfr. art. 4, comma 1, lett. *i*)[23]. «Titolare» è, invece, la

[21] Secondo la giurisprudenza costituiscono dato personale: il numero di telefono cellulare (Cass., sez. III, 23 ottobre 2008, in «Ced Cass.», rv. 241787); le generalità e l'indirizzo di una persona (Trib. Roma, 10 gennaio 2003, in «Dir. informazione e informatica», 2003, 532); la valutazione espressa in sede di perizia medico-legale (Trib. Roma, 17 luglio 2003, in «Guida al dir.», 2003, fasc. 50, 36); una lettera con la quale il mittente domandi al destinatario il risarcimento di un danno per presunto illecito commesso dal secondo nei confronti del primo (Cass., sez. III, 24 aprile 2008, n. 10690, in «Dir. informazione e informatica», 2008, 495); i dati relativi alle ore di straordinario dei dipendenti (Trib. Torino, 26 settembre 2000, in «Giur. piemontese», 2001, 159); la valutazione finale del dipendente attribuita dal datore di lavoro (Trib. Fermo, 26 ottobre 1999, in «Notiziario giurisprudenza lav.», 1999, 626).

[22] Secondo Cass., sez. lav., 7 luglio 2008, n. 18584, in «Foro it.», Rep. 2008, voce «Persona fisica», n. 107, non costituisce dato sensibile, ma mero dato personale, la semplice appartenenza alla clientela di un medico specialista del soggetto chiamato a deporre in un giudizio. Una disciplina particolare è dettata anche per i «dati giudiziari», ovvero i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lett. da *a* a *o*, e da *r* a *u*, d.p.r. 313/2002, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del codice di procedura penale (cfr. art. 4, comma 1, lett. *e*).

[23] Secondo Cass., 8 luglio 2005, n. 14390, in «Foro it.», 2007, I, 511, per assumere la qualità di «interessato» non è richiesto che i dati appartengano, con certezza, alla persona che si duole delle operazioni compiute su di essi, mentre rileva la loro attribuzione o la loro esclusione rispetto a colui che, al riguardo, accampi un diritto (alla titolarità, ovvero all'estraneità, dei medesimi).

persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza (cfr. art. 4, comma 1, lett. *f*). Il titolare può preporre al trattamento dei dati personali dei «responsabili», che possono essere persone fisiche o giuridiche, ovvero pubbliche amministrazioni o qualsiasi altro ente, associazione o organismo (cfr. art. 4, comma 1, lett. *g*). Titolari o responsabili possono autorizzare persone fisiche a compiere operazioni di trattamento: la figura prende il nome di «incaricato» (cfr. art. 4, comma 1, lett. *h*).

Il codice riconosce all'interessato una serie di diritti. Essi sono:

- diritto di conoscenza[24];
- diritto di accesso ai dati[25];
- diritto di modifica e aggiornamento di dati incompleti o obsoleti[26];
- diritto all'oblio (cancellazione dei dati non più necessari in relazione ai fini per i quali erano stati raccolti)[27];
- diritto di opporsi al trattamento[28].

[24] Cfr. art. 7, comma 1, del codice della privacy: l'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. Per una fattispecie in materia di documentazione relativa a lavoratori cfr. Cass., sez. lav., 26 aprile 2007, n. 9961, in «Notiziario giurisprudenza lav.», 2007, 353.

[25] Ai sensi dell'art. 7, comma 2, del codice della privacy, l'interessato ha diritto di ottenere l'indicazione: *a*) dell'origine dei dati personali; *b*) delle finalità e modalità del trattamento; *c*) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; *d*) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5, comma 2; *e*) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

[26] Cfr. art. 7, comma 3, del codice della privacy: l'interessato ha diritto di ottenere l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati.

[27] Cfr. art. 7, comma 3, del codice della privacy: l'interessato ha diritto di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati. L'interessato ha anche diritto di ottenere l'attestazione che le operazioni appena ricordate (aggiornamento, cancellazione, ecc.) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

[28] Secondo l'art. 7, comma 4, del codice della privacy, l'interessato ha diritto di opporsi, in tutto o in parte: *a*) al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta, se esistono motivi legittimi; *b*) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato

I diritti appena elencati possono essere esercitati secondo le modalità previste negli artt. 8, 9 e 10 del codice.

Principi generali vengono dettati in ordine alle modalità di trattamento. In particolare i dati personali oggetto di trattamento devono essere:

– trattati in modo lecito e secondo correttezza;

– raccolti e registrati per scopi determinati, espliciti e legittimi, e utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

– esatti e, se necessario, aggiornati;

– pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

– conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati (cfr. art. 11 del codice).

La raccolta di dati personali deve essere di regola preceduta da un'informativa fornita, oralmente o per iscritto, all'interessato che contenga una serie di informazioni tra le quali (cfr. art. 13 del codice):

– le finalità e le modalità del trattamento cui sono destinati i dati;

– la natura obbligatoria o facoltativa del conferimento dei dati;

– le conseguenze di un eventuale rifiuto di rispondere;

– i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

– i diritti di cui all'art. 7, prima ricordati;

– gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato e del responsabile.

In linea di principio il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato che può riguardare l'intero trattamento ovvero una o più operazioni dello stesso. Il consenso è validamente prestato solo se è espresso

o di comunicazione commerciale. In argomento cfr. Cass., 15 luglio 2005, n. 15076, in «Guida al dir.», 2005, fasc. 31, 37.

liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'art. 13. Quando il trattamento riguarda dati sensibili il consenso è manifestato in forma scritta (cfr. art. 23 del codice); il successivo art. 24 elenca, però, le ipotesi in cui si può procedere a trattamento anche senza consenso (ad esempio quando il trattamento è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria).

3. L'ENFASI SULLA SICUREZZA

L'accento posto sulla protezione dei dati personali costituisce la naturale evoluzione di un altro elemento che caratterizza la produzione normativa in tema di *computer privacy*: l'esigenza che il trattamento dei dati avvenga in un contesto di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza. Nel considerando n. 46 della direttiva 1995/46/CE si legge:

> la tutela dei diritti e delle libertà delle persone interessate relativamente al trattamento di dati personali richiede l'adozione di adeguate misure tecniche ed organizzative sia al momento della progettazione che a quello dell'esecuzione del trattamento, in particolare per garantirne la sicurezza ed impedire in tal modo qualsiasi trattamento non autorizzato; [...] spetta agli Stati membri accertarsi che il responsabile del trattamento osservi tali misure; [...] queste devono assicurare un adeguato livello di sicurezza, tenuto conto delle conoscenze tecniche e dei costi dell'esecuzione rispetto ai rischi che i trattamenti presentano e alla natura dei dati da proteggere.

Muovendo da quanto prescritto nella sezione VIII della direttiva 1995/46/CE, il codice della privacy impone al titolare del trattamento di osservare alcuni obblighi atti a garantire la sicurezza. In particolare l'art. 31 prevede che i dati personali debbano essere custoditi e controllati in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei

dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta: tutto ciò deve avvenire mediante l'adozione di idonee e preventive misure di sicurezza che facciano riferimento alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento[29]. La disciplina interessa i soggetti pubblici e privati, comprese le persone fisiche che trattano dati per fini non esclusivamente personali che non sono soggette a nessun altro obbligo del codice: chiunque gestisca un archivio contenente dati personali altrui sarà responsabile del rischio di perdita o distruzione, anche accidentale (art. 5 del codice). Questa previsione si ricollega al principio generale dell'interesse all'integrità e alla completezza dei dati.

A ben vedere l'art. 31 appena richiamato non specifica la nozione di «misure di sicurezza idonee e preventive»: è il prezzo pagato al continuo variare delle tecnologie che rende poco lungimirante il riferimento a specifiche misure destinate a rivelarsi obsolete o non efficaci. Manca, peraltro, qualsiasi riferimento ai costi nell'implementazione, che invece la direttiva 1995/46/CE prevedeva all'art. 17. Tale scelta rende l'impianto delle misure di sicurezza nel contesto nazionale maggiormente restrittivo rispetto al contesto europeo, perché non prevede la possibilità di una maggiore modularità di implementazione delle misure stesse.

Chi tratta dati personali deve comunque porre in essere «misure minime di sicurezza» ovvero un complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art. 31 (art. 4, comma 3, lett. *a*). Il codice fa riferimento a fattori ed eventi di rischio di diversa importanza e causalità, che dipendono da varie condizioni interne ed esterne, nei confronti delle quali assume estrema importanza il complesso degli strumenti e dei metodi adottati in via preventiva nel contesto delle operazioni di trattamento. Maggiore sarà il rischio che può derivare da intromissioni esterne o da possibili interventi sui dati personali, tanto più deve ritenersi vincolante l'adozione di strumenti e metodologie di prevenzione o di riduzione del rischio [Guarda 2008].

[29] L'allegato B al codice della privacy contiene il disciplinare tecnico in materia di misure minime di sicurezza [Perri 2007; Caso 2006].

In particolare l'art. 34 del codice sancisce che il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B, le seguenti misure minime:

a) l'autenticazione informatica, ovvero l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità; il ricorso ad essa evita che esistano trattamenti di dati effettuati con strumenti elettronici che non siano correttamente riferibili ad uno specificato incaricato;

b) l'adozione di procedure di gestione delle credenziali di autenticazione. Costituiscono credenziali di autenticazione i dati e i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica[30];

c) l'utilizzazione di un sistema di autorizzazione, ovvero dell'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente[31];

d) l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) l'adozione di procedure per la custodia di copie di sicurezza e per il ripristino della disponibilità dei dati e dei sistemi;

g) la tenuta di un aggiornato documento programmatico sulla sicurezza[32];

h) l'adozione di tecniche di cifratura o di codici identificativi per tratta-

[30] L'allegato B al codice spiega che esse consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

[31] Per profilo di autorizzazione si intendono le informazioni, univocamente associate ad una persona, che consentono di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

[32] L'art. 29, comma 1, d.l. 25 giugno 2008, n. 112, come modificato dalla relativa legge di conversione, prevede che la tenuta del documento programmatico sulla sicurezza sia sostituita dall'obbligo di autocertificazione per i soggetti che trattano soltanto dati personali non sensibili ovvero un numero qualitativamente e quantitativamente circoscritto di dati sensibili.

menti, effettuati da organismi sanitari, idonei a rivelare lo stato di salute o la vita sessuale.

La concreta applicazione di queste regole e i significati dei termini tecnici appena richiamati sono contenuti nel disciplinare tecnico in materia di misure minime di sicurezza (contenuto nell'allegato B al codice).

La violazione dell'obbligo di adottare le misure minime di sicurezza (delineate nell'art. 33 del codice della privacy) è sanzionata penalmente (cfr. art. 169, d.lgs. 196/2003)[33]. Sul piano civilistico, il trattamento dei dati personali è considerato esercizio di attività pericolosa. Infatti, a norma dell'art. 15 del codice, chiunque cagioni danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'art. 11 che elenca i principi, già ricordati, in tema di modalità del trattamento dei dati e requisiti dei medesimi[34].

Alla diffusione sempre più capillare dei computer fa eco una crescente ansia di sicurezza, alimentata dalla consapevolezza della:

- possibile utilizzazione maliziosa e dannosa dei dati personali che riguardano gli individui (e i soggetti diversi dalle persone fisiche): la casistica sviluppatasi successivamente all'emanazione della legge sulla privacy contempla le indagini sulla solvibilità svolte illecitamente[35]; la pubblicazione su un quotidiano dell'immagine altrui senza il consenso dell'interessato[36]; la circolazione di informazioni relative all'appartenenza a un sindacato[37]; la pubblicazione, senza il consenso degli interessati, dei dati

[33] Chiunque, essendovi tenuto, ometta di adottare le misure minime previste dall'art. 33 è punito con l'arresto sino a due anni. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento. In ogni caso il termine non può superare i sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli artt. 21, 22, 23 e 24, d.lgs. 758/1994 in quanto applicabili.

[34] Per la statuizione del principio cfr. la massima di Cass., sez. un., 11 novembre 2008, n. 26972, in «Resp. e risarcimento», 2008, fasc. 11, 14.

[35] Trib. Orvieto, 25 novembre 2002, in «Danno e resp.», 2003, 281.

[36] Trib. Biella, 29 marzo 2003, in «Dir. informazione e informatica», 2003, 538.

[37] Trib. Palermo, 12 giugno 2001, in «Foro it.», 2001, I, c. 2982.

riguardanti la residenza e il numero telefonico[38]; l'invio da parte di un gestore del servizio di telefonia mobile, al proprio cliente, titolare di una scheda prepagata, senza il suo consenso e malgrado l'opposizione dallo stesso manifestata, di alcuni sms contenenti informazioni relative a servizi collegati con l'uso del telefono cellulare che, pur potendo essere abilitati gratuitamente, sono a pagamento[39]; l'invio di una comunicazione relativa alla presentazione di una domanda di pensione per invalidità, contenente anche la notizia di una visita medica, tramite una cartolina aperta[40]; la mancata adozione da parte dell'editore delle misure minime atte a garantire l'inaccessibilità agli altri membri della redazione della posta elettronica inviata personalmente ad un singolo giornalista[41]; la mancata adozione di accorgimenti che impediscano l'identificazione del soggetto affetto da una patologia contagiosa che richieda accertamenti sanitari sui colleghi[42]; l'utilizzo di dati personali illecitamente trattati da parte di una banca come forma di coazione psicologica per ottenere l'adempimento di un proprio debitore moroso[43]; il rilascio da parte di un medico di una dichiarazione inerente alle condizioni di salute psichica di una persona da lui visitata a soggetto diverso dall'interessato, e senza il consenso del paziente[44]; la diffusione di dati sensibili contenuti in una cartella clinica[45]; la comunicazione da parte del curatore di un fallimento ai soci di un circolo di vantare un credito nei confronti di un socio[46];

- dipendenza sempre maggiore delle società avanzate dai sistemi informatici e telematici: nel considerando n. 1 del regolamento CE 460/2004 si legge:

[38] Trib. Milano, 19 maggio 2005, in «Danno e resp.», 2006, 1247.

[39] Trib. Latina-Terracina, 19 giugno 2006, in «Foro it.», 2007, I, 324.

[40] Giudice di pace Bari, 12 dicembre 2005, in «Foro it.», Rep. 2006, voce «Persona fisica», n. 104.

[41] Giudice di pace Bari, 7 giugno 2005, in «Dir. Internet», 2005, 573.

[42] App. Milano, 19 giugno 2007, in «Dir. informazione e informatica», 2007, 1101.

[43] Trib. Venezia, 20 giugno 2005, in «Danno e resp.», 2006, 666.

[44] Trib. Milano, 8 agosto 2003, in «Danno e resp.», 2004, 303.

[45] Cass., sez. III, 30 gennaio 2009, n. 2468, in «Giust. civ.», 2009, I, 885.

[46] Trib. Roma, 6 dicembre 2002, in «Dir. informazione e informatica», 2003, 339.

> Le reti di comunicazione e i sistemi di informazione sono ormai fattori determinanti dello sviluppo economico e sociale. Computer e reti stanno diventando strumenti altrettanto comuni dell'acqua corrente o dell'energia elettrica. La sicurezza delle reti di comunicazione e dei sistemi di informazione, in particolare la loro disponibilità, diventa di conseguenza sempre più importante per la società anche a causa della possibilità che si presentino problemi nei sistemi chiave d'informazione a motivo della complessità del sistema, di incidenti, errori e attacchi che possono avere conseguenze sulle infrastrutture fisiche che forniscono servizi essenziali per il benessere dei cittadini dell'UE[47];

• vulnerabilità dei sistemi: nel considerando n. 2 del regolamento appena citato si legge:

> Il numero crescente di violazioni della sicurezza ha già provocato notevoli danni economici, turbato la fiducia degli utenti e danneggiato lo sviluppo del commercio elettronico. Gli individui, le amministrazioni pubbliche e le imprese hanno reagito dotandosi di tecnologie e procedure di gestione relative alla sicurezza. Gli Stati membri hanno preso a loro volta numerose misure di sostegno per accrescere la sicurezza delle reti e dell'informazione nella società, come ad esempio campagne di informazione e progetti di ricerca[48].

(Sul rapporto tra privacy e commercio elettronico si tornerà nelle pagine successive.) Ansia di sicurezza dunque. Ma un particolare merita di essere sottolineato. Nella normativa qui ricordata, a cominciare dalla direttiva

[47] Regolamento CE 460/2004 del Parlamento europeo e del Consiglio del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione. Corte giustizia Comunità europee, 2 maggio 2006, n. 217/04, in «Raccolta», 2006, I, p. 3771 ha chiarito, tra l'altro, che i compiti affidati all'Agenzia sono strettamente connessi agli obiettivi perseguiti dalla direttiva 2002/21/CE (quadro normativo comune per le reti e i servizi di comunicazione elettronica esaminata nell'Introduzione), e dalle direttive speciali nel settore della sicurezza delle reti e dell'informazione e che il regolamento non costituisce un provvedimento isolato, iscrivendosi invece in un contesto normativo delimitato dalla direttiva 2002/21 nonché dalle direttive speciali relative alle reti e alle comunicazioni elettroniche, diretto alla realizzazione del mercato interno nel settore delle comunicazioni elettroniche: trovandosi di fronte a una materia che implica tecnologie non soltanto complesse, ma altresì in rapido mutamento, il legislatore comunitario ha ritenuto che l'istituzione di un organismo comunitario quale l'Agenzia fosse un mezzo adeguato per prevenire l'insorgere di disparità potenzialmente idonee a creare ostacoli al buon funzionamento del mercato interno in materia.

[48] *Ibidem*.

1995/46/CE, la parola «sicurezza» (o il corrispondente *security*, nel testo inglese di quell'atto) è utilizzata tanto per indicare la necessità di tutelare i dati personali trattati al fine di garantirne al meglio la riservatezza, quanto per individuare gli interessi la cui tutela può giustificare una protezione meno stringente della privacy dei cittadini: si veda il riferimento alla sicurezza nazionale e alla sicurezza pubblica contenuto nell'art. 13 della direttiva 1995/46/CE[49]. Si ribadirà nel prosieguo che tutelare la privacy significa, spesso, individuare i confini con la tutela di altri interessi che con la stessa possono confliggere. Qui conviene ricordare che dopo l'11 settembre 2001 (attacco alle Torri gemelle di New York) si sono moltiplicate le iniziative legislative volte a contrastare il terrorismo internazionale. Per gli Stati Uniti si veda il *Patriot Act* (USAPA, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*) del 26 ottobre 2001 teso ad ampliare, tra l'altro, i poteri di intercettazione e sorveglianza alle autorità federali [De Petris 2007]. Come è evidente, tali misure possono interferire con la privacy dei cittadini[50].

[49] Il testo dell'art. 13 recita: «1. Gli Stati membri possono adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti dalle disposizioni dell'art. 6, paragrafo 1, dell'art. 10, dell'art. 11, paragrafo 1, e degli artt. 12 e 21, qualora tale restrizione costituisca una misura necessaria alla salvaguardia: *a*) della sicurezza dello Stato; [...] *c*) della pubblica sicurezza». Cfr. anche l'art. 15 della direttiva 2002/58/CE.

[50] Per il Regno Unito cfr. l'*Anti-Terrorism, Crime and Security Act* del 2001. In Italia il d.l. 27 luglio 2005, n. 144 – Misure urgenti per il contrasto del terrorismo internazionale, convertito in legge 31 luglio 2005, n. 155, tra le altre misure, aveva prolungato i termini di conservazione dei dati relativi al traffico telefonico o telematico. In argomento è poi intervenuto il d.lgs. 30 maggio 2008, n. 109, che ha dato attuazione alla direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione. Tale decreto ha tra l'altro modificato l'art. 132 del codice della privacy, il cui comma 1 recita: «Fermo restando quanto previsto dall'art. 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data di comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione». I dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore, i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'art. 391-*quater* del codice di procedura penale, ferme restando le condizioni di cui all'art. 8, comma 2, lett. *f*, per il traffico entrante. Sono state sollevate alcune questioni di legittimità costituzionale della norma in parola che però la Consulta ha dichiarato inammissibili o infondate con sentenza 14 novembre 2006, n. 372, in «Dir. e giustizia», 2006, fasc. 44, 59. L'art. 3, d.lgs. 109/2008 elenca le tipologie di dati che devono essere conservati dagli operatori di telefonia e di comunicazione elettronica per le finalità di cui al citato art. 132 del codice della privacy. Sul punto è anche intervenuto l'art. 12-*ter*, d.l. 23 febbraio 2009, n. 11, recante

4. LA RISERVATEZZA NELL'ERA DI INTERNET

Nel parlare di vulnerabilità dei sistemi informatici si è fatto riferimento (citando il regolamento CE 460/2004) al rapporto tra privacy e commercio elettronico. Il tema merita di essere approfondito. La metà degli anni '90 segna il definitivo affermarsi di Internet[51]. Il numero di computer interconnessi cresce in maniera esponenziale, la rete si apre alle famiglie e alle imprese commerciali. Tutta l'attività compiuta in rete può essere monitorata. Partiamo da due esempi: *cookies* e *logs*.

4.1. «Logs» e «cookies»

Un *log* è un file di testo in cui viene registrata e documentata l'attività di applicazioni software installate su un computer. Un file *log* è automaticamente generato presso il fornitore di accesso ad Internet (*provider*) e documenta tutta l'attività che il singolo navigatore ha svolto sulla rete durante il collegamento. Grazie ai *logs* il gestore di un sito può conoscere quanti sono i visitatori, quando arrivano, da dove vengono (e in molti casi anche chi sono), cosa fanno, quanto si fermano e quali pagine consultano. Spesso nei *logs* sono registrate informazioni assai dettagliate che consentono di ricostruire un profilo preciso del navigatore[52].

misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori convertito nella legge 38/2009 che ha introdotto nel nostro ordinamento il reato di *stalking*: art. 612-*bis* del codice penale.

[51] Samuelson [1999, 766] scrive: «It's fair to observe, however, that the data privacy rights [...] are not privacy rights in the classic "right to be let alone" sense [...] some might argue that they really are not even privacy interests at all».

[52] Tale profilo si rivela utilissimo per effettuare promozioni commerciali, in quanto consente di indirizzare in modo mirato un determinato messaggio pubblicitario, sia tramite e-mail, sia attraverso mezzi più tradizionali. Utilizzando uno strumento come *Shinystat* (http://www.shinystat.com/it) si può monitorare la propria homepage per conoscere, ad esempio, indirizzo IP del visitatore, orario di visita, pagine visitate, sistema operativo installato, risoluzione video, tipologia di *browser* utilizzato. Trib. Chieti, 30 maggio 2006, in «Dir. Internet», 2006, 572, si è occupato della rilevanza dei file *log* nel processo penale sostenendo che «le attività di apprensione dei file di *log* da parte della polizia giudiziaria devono essere accompagnate da un attento controllo circa le modalità di conservazione dei dati informatici, allo scopo di verificare l'assenza di manipolazioni e la conseguente genuinità delle evidenze digitali; in mancanza di tali inadempimenti, i file di *log*, specie ove provengano dalla stessa persona offesa, costituiscono materiale del tutto insufficiente a fondare qualsivoglia affermazione di responsabilità al di là del ragionevole dubbio». Il problema rinvia alla c.d. *computer forensics* di cui si parlerà nel capitolo dedicato all'informatica nel processo penale.

I *cookies* (biscottini) sono file di piccole dimensioni, normalmente in formato ASCII, che contengono informazioni di base relative ad un utente in relazione ad un *server*. Ogni volta che l'utente accede ad un determinato sito Internet, quest'ultimo può inviare un *cookie* al fine di ottenere alcuni dati. I *cookies*, infatti, consentono al *server* di scrivere in modo permanente alcune informazioni sulla macchina *client* (cioè sul computer dell'utente), in modo che possano essere disponibili in successive sessioni di collegamento[53]. Le informazioni contenute in un *cookie* consistono, generalmente, in dati relativi al *login*, ad eventuali registrazioni, ad acquisti in linea, ecc. I *cookies* vengono utilizzati per controllare con quale frequenza il navigatore accede al sito, per personalizzare il sito, per evitare una nuova autenticazione, per definire il profilo dell'utente in ragione delle pagine maggiormente visitate[54].

4.2. Una nuova ragione per tutelare la privacy

Nella seconda metà degli anni '90, con l'esplosione del World Wide Web e dei *browsers* di navigazione (Netscape e Internet Explorer), la rete diventa strumento per vendere beni e servizi vecchi e nuovi (commercio

[53] I *cookies* sono presi in considerazione dall'art. 5, comma 3, della direttiva 2002/58/CE, come sostituito dall'art. 2, n. 5, della direttiva 2009/136/CE che (alla luce di quanto sancito nel considerando n. 66) così recita: «Gli Stati membri assicurano che l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva 1995/46/CE, tra l'altro sugli scopi del trattamento. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio».

[54] Ad esempio, quando si acquista via Internet, normalmente si naviga tra le pagine che presentano i vari prodotti e, quando se ne trova uno interessante, lo si inserisce nel «carrello della spesa virtuale»; il *server* invia al *browser* un *cookie*, che contiene l'indicazione del prodotto scelto. Da quel momento, ogni volta che sarà richiamata una pagina dello stesso sito, il *browser* segnalerà al *server* che è già stato selezionato tale oggetto, rispedendogli il *cookie*; in questo modo, esso potrà sapere in ogni momento che cosa è stato selezionato. Ogni *cookie* è strettamente legato al sito che lo ha emesso e può essere interpretato correttamente solo da quello. Tuttavia, in linea di principio, non si può escludere che le informazioni contenute nel *cookie* vengano memorizzate e utilizzate a discrezione del titolare del sito web emittente.

elettronico). Ci si rende conto che il decollo di siffatte attività sulla rete può essere seriamente ostacolato se i potenziali clienti dovessero sentirsi minacciati da imprecisati rischi derivanti dall'incontrollabile diffusione di informazioni riguardanti la propria sfera privata[55]. La fiducia è un elemento fondamentale del successo della nuova società dell'informazione[56]. Proprio per accrescere la fiducia dei consumatori nel commercio elettronico, l'Unione europea ha varato il progetto *E-confidence*[57].

Inutile dire che la rilevanza del tema è stata colta per tempo anche oltre Atlantico. Nel rapporto denominato *Options for Promoting Privacy on the National Information Infrastructure* della National Information Infrastructure Task Force – Information Policy Committee, datato aprile 1997, si legge testualmente:

> I consumatori vogliono controllare quali dati personali che li riguardano vengono diffusi, a chi, e come quelle informazioni saranno usate. Di conseguenza, il commercio elettronico fiorirà solo se sapremo concordare e applicare pratiche leali di trattamento dei dati nella società dell'informazione[58].

[55] Conferma di quanto esposto nel testo si trova nei considerando nn. 5, 6 e 7 della direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 (direttiva relativa alla vita privata e alle comunicazioni). La direttiva 2009/136/CE, che ha introdotto alcune modifiche alla direttiva appena citata, stigmatizza in maniera ancora più puntuale i rischi richiamati nel testo. Nel considerando n. 61 si legge, infatti: «Una violazione di dati personali può, se non è trattata in modo adeguato e tempestivo, provocare un grave danno economico e sociale, tra cui l'usurpazione d'identità, all'abbonato o alla persona interessata. Pertanto, il fornitore di servizi di comunicazione elettronica accessibili al pubblico, non appena viene a conoscenza del fatto che si è verificata tale violazione, dovrebbe notificarla all'autorità nazionale competente. È opportuno che gli abbonati o le persone i cui dati e la cui vita privata potrebbero essere pregiudicati da tali violazioni siano informati tempestivamente per permettere loro di adottare le precauzioni necessarie. Si considera che una violazione pregiudica i dati o la vita privata di un abbonato o di una persona quando implica, ad esempio, il furto o l'usurpazione d'identità, il danno fisico, l'umiliazione grave o il danno alla reputazione in relazione con la fornitura di servizi di comunicazione accessibili al pubblico nella Comunità. È opportuno che la comunicazione includa informazioni sulle misure adottate dal fornitore per affrontare la violazione così come raccomandazioni per gli abbonati o le persone coinvolti».

[56] Cfr. risoluzione del Consiglio del 22 marzo 2007 su una strategia per una società dell'informazione sicura in Europa, punto n. 2

[57] Sul punto cfr. Commissione dell'Unione europea, *Consumer Confidence in E-commerce: Lessons Learned from the E-confidence Initiative*, Bruxelles, 8 novembre 2004, SEC(2004)1390, http://ec.europa.eu/consumers/cons_int/e-commerce/e-conf_working_doc.pdf.

[58] Il documento è ancora accessibile al seguente indirizzo: www.empowermentzone.com/nii_priv.txt. Del pari, nel resoconto del *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, curato dalla Federal Trade Commission (dicembre 1996), consultabile all'indirizzo http://www.ftc.gov/reports/privacy/privacy.pdf, si legge: «The proliferation of readily available personal information, however, also could jeopardize personal privacy and facilitate fraud and deception. These risks may make consumers reluctant to use the Internet or participate in on-line transactions and therefore could prevent consumers from obtaining the benefits promised by on-line commerce».

Per certi versi si assiste ad un paradosso. Interessato a raccogliere dati personali è colui che offre i servizi sulla rete. E la sua attività sarà tanto più redditizia quanto più il cliente si fiderà di lui [Guarda 2004]. E il cliente si fiderà, tra l'altro, se saprà che non corre alcun rischio derivante da un uso improprio dei suoi dati[59]. In linea di principio è interesse di chi raccoglie i dati garantire un alto standard di tutela al titolare dei dati stessi[60]. La reputazione delle compagnie (con la connessa capacità di imporsi sul mercato) è destinata a soffrire se non si trova il modo di soddisfare i desideri dei consumatori in ordine alla tutela dei dati personali.

Chi raccoglie i dati non è animato dall'obiettivo di discriminare qualcuno: si trattano informazioni per «servire» meglio i clienti. I ritrovati utili a creare dei profili dei navigatori della rete (ad esempio *cookies* e *logs*) mirano a conoscere i gusti degli utenti per offrire prodotti e servizi in maniera

[59] Sempre più spesso la posta elettronica viene usata per recapitare valanghe di messaggi in serie che pubblicizzano prodotti e servizi. Tale attività, detta *spamming*, è disciplinata dall'art. 130 del codice della privacy come modificato dall'art. 20-*bis*, legge 166/2009 che ha convertito il d.l. 135/2009, con il quale è stata data attuazione, in *parte qua*, alla direttiva 2002/58/CE. In linea di principio l'inoltro automatico (ovvero senza operatore) di e-mail per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato. Peraltro l'art. 2, n. 7, della direttiva 2009/136/CE ha sostituito l'art. 13 della direttiva 2002/58/CE. Un elemento significativo della novella è rappresentato dalla possibilità riconosciuta ai fornitori di servizi di posta elettronica e agli altri fornitori di servizi di promuovere azioni giudiziarie contro gli *spammers* sul presupposto che la difesa degli interessi dei clienti è parte integrante della tutela dei propri interessi commerciali (cfr. il considerando n. 68 della nuova direttiva). La scelta riposa anche sulla consapevolezza che i fornitori di servizi di comunicazione elettronica possiedono le conoscenze e le risorse necessarie per individuare e identificare coloro che inviano tali comunicazioni commerciali indesiderate. In argomento cfr. Giudice di pace Napoli, 10 giugno 2004, in «Foro it.», 2004, I, c. 2908 (a cui dire l'invio di posta elettronica indesiderata costituisce fatto illecito produttivo di responsabilità civile sia per la scorrettezza e l'illiceità del trattamento dei dati personali del titolare dell'indirizzo bersaglio, sia per l'invasione della sfera di riservatezza di quest'ultimo); nonché Tribunal de commerce, Paris, 5 maggio 2004, in «Foro it.», 2004, IV, c. 510; Trib. Prato, 15 ottobre 2001, in «Giur. merito», 2002, p. 354.

[60] Va da sé che le cose non stanno necessariamente così. Spesso c'è sproporzione tra chi offre e chi accetta servizi sulla rete. Chi offre servizi in regime di quasi monopolio (si pensi all'offerta anche gratuita dell'aggiornamento di un sistema operativo molto diffuso) può pretendere dati personali senza nei fatti essere obbligato a garantire un qualsivoglia livello di tutela per quei dati: l'utente che avendo installato il software ha necessità dell'*upgrade*, di un accessorio o di un *plug-in*, accetterà comunque di fornire dati pur di scaricare quello che gli serve.

mirata[61]. Sotto questo aspetto i dati personali (*rectius*: gusti) assumono una rilevanza economica.

Riprova di quanto appena affermato può essere considerata la prassi adottata dai principali Internet *providers* di offrire gratuitamente agli utenti l'accesso alla rete (c.d. *free-web*). Il paradigma è quello del baratto in cui si scambia l'attenzione per la comunicazione commerciale con beni e servizi gratuiti. Scompare il canone, ma il «prezzo» rimane anche se non è visibile immediatamente. Gli utenti «pagano» in due modi: fornendo utili informazioni circa i propri gusti ed abitudini e generando traffico telefonico.

Nel contratto di accesso gratuito ad Internet predisposto da Wind si legge testualmente[62]:

> 6. Profilazione – Per profilazione si intende il processo mediante il quale possono essere rilevate le attitudini commerciali del cliente manifestate attraverso le navigazioni. Wind adotterà un sistema di profilazione degli utenti basato sull'analisi degli accessi ad una lista predefinita di siti che meglio rappresentano gli interessi del cliente da un punto di vista strettamente ed esclusivamente commerciale. La lista si compone dei siti web più rappresentativi delle diverse categorie merceologiche. Tali siti saranno scelti fra i più popolari e stabili per ogni categoria merceologica. Il catalogo così definito sarà mantenuto aggiornato e verrà periodicamente verificato da Wind. Wind, mediante il sistema di formazione e conservazione del suddetto catalogo, assicura e garantisce che il suddetto catalogo non comprenderà siti nei quali siano trattati in maniera diretta o indiretta argomenti riguardanti dati sensibili: «[...] l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale [...]» ai sensi dell'art. 20 del d.lgs. 196/2003. Pertanto verrà escluso *a priori* ogni trattamento che possa riguardare direttamente o indirettamente dati sensibili[63].

[61] Un elenco assolutamente incompleto di tipologie di dati che possono rivestire interesse per fornitori di beni e servizi comprende: dati sanitari, transazioni bancarie, storia del ricorso al credito, telefonate locali o a lunga distanza, *Pay per view*, acquisto o noleggio di videocassette, acquisti via Internet, dati posseduti dai *service providers*.

[62] Cfr. http://registrazione.libero.it/comscripts/viewdoc.php?name=contratto.html. Nell'informativa che Wind fornisce ai clienti ai sensi dell'art. 13 del codice della privacy si legge che i dati vengono trattati per le seguenti finalità: «*a.* raccolta e conservazione dei Suoi dati personali al fine della fornitura del servizio [...] e per fornire all'Autorità giudiziaria le informazioni richieste; *b.* elaborazione dei dati personali da Lei forniti e di quelli desunti dalle Sue navigazioni in rete, in base al processo meglio chiarito nelle condizioni generali di servizio, allo scopo di definire il Suo profilo commerciale; *c.* utilizzo del Suo profilo commerciale da parte di [...] per finalità di marketing e promozionali proprie di [...]; *d.* raccolta, conservazione ed elaborazione dei Suoi dati personali per scopi amministrativo-contabili, compresa l'eventuale trasmissione per posta elettronica di fatture commerciali; *e.* comunicazione del Suo profilo commerciale a [...] per fini di marketing e promozionali propri di [...]; *f.* utilizzo del Suo profilo commerciale da parte di [...] e [...] per finalità di marketing e promozionali di terzi».

4.3. Le regole della rete e i codici di condotta

Con l'esplosione di Internet sorge la necessità di capire se sono applicabili alla rete (e ai nuovi strumenti tecnologici dalla stessa introdotti, ad esempio *cookies* e *logs*) le normative emanate di volta in volta per disciplinare il trattamento di dati personali. La complicazione deriva dall'estrema facilità con la quale si lasciano in giro informazioni e dal carattere aterritoriale della rete che rende estremamente facile aggirare le discipline più restrittive, a tacere della difficoltà di assicurare l'*enforcement* delle disposizioni poste a tutela dell'individuo.

Il problema del regime applicabile al trattamento dei dati personali sulla rete rinvia ad un tema più generale relativo all'approccio più idoneo a governare la rete[64]. Sul punto conviene spendere qualche parola.

[63] Sul tema si veda il provvedimento del Garante per la protezione dei dati personali del 25 giugno 2009, recante «Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione» (GU n. 159 dell'11 luglio 2009).

[64] In argomento cfr. la raccomandazione N.R. (99) 5 del Comitato dei ministri del Consiglio d'Europa agli Stati membri per la protezione della privacy su Internet. La raccomandazione è significativa, anche in relazione al periodo in cui è stata emanata, perché: *a)* non sceglie come interlocutori i soggetti tradizionalmente deputati alla produzione delle regole (ad esempio i legislatori nazionali) bensì i soggetti direttamente interessati e coloro che possono in concreto garantire il rispetto della privacy degli utenti assicurando una gestione corretta dei dati (ovvero: utenti da un lato e fornitori di accesso ad Internet dall'altro); *b)* non auspica il ricorso a norme cogenti eteroimposte ma invita gli stessi interessati a dotarsi di codici di condotta che incorporino talune *Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways*, che la stessa raccomandazione contiene. Ad esempio, rivolgendosi agli utenti di Internet le *Guidelines* recitano: «Ricorda che Internet non è sicura. Usa tutti i mezzi tecnici idonei a proteggere dati personali e comunicazioni, come ad esempio i sistemi di crittografia» (App. II, 1); oppure: «Ricorda che ogniqualvolta fai una transazione o visiti un sito su Internet lasci delle tracce. Queste tracce

L'art. 27 della direttiva 1995/46/CE del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, incoraggia gli ambienti professionali interessati ad elaborare codici di condotta destinati a favorire, secondo le caratteristiche specifiche dei trattamenti effettuati in taluni settori, l'attuazione della direttiva nel rispetto delle disposizioni nazionali di applicazione della stessa[65].

L'input comunitario è stato raccolto in Italia dall'art. 133 del codice sulla privacy che recita:

> Il Garante promuove, ai sensi dell'art. 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato da fornitori di servizi di comunicazione e informazione offerti mediante reti di comunicazione elettronica, con particolare riguardo ai criteri per assicurare ed uniformare una più adeguata informazione e consapevolezza degli utenti delle reti di comunicazione elettronica gestite da soggetti pubblici e privati rispetto ai tipi di dati personali trattati e alle modalità del loro trattamento, in particolare attraverso informative fornite in linea in modo agevole e interattivo, per favorire una più ampia trasparenza e correttezza nei confronti dei medesimi utenti e il pieno rispetto dei principi di cui all'art. 11, anche ai fini dell'eventuale rilascio di certificazioni attestanti la qualità delle modalità prescelte e il livello di sicurezza assicurato.

È utile chiedersi la ragione del risalto dato ai codici deontologici [Alpa e Zatti 2006]. Forse una risposta può venire muovendo da alcune riflessioni innescate dal modo di atteggiarsi della tutela della privacy nell'ambito dell'attività giornalistica[66].

elettroniche possono essere usate, a tua insaputa, per costruire un profilo della tua persona e dei tuoi interessi. Se non vuoi che ciò avvenga sei invitato a fare uso degli ultimi ritrovati tecnologici che includono la possibilità di essere informato ogni volta che stai lasciando delle tracce e di rifiutare che ciò avvenga. Puoi anche chiedere informazioni sulla politica in materia di privacy (*privacy policy*) adottata dai diversi siti e dare la preferenza a quei siti che raccolgono pochi dati e possono essere visitati in forma anonima» (App. II, 2); o ancora: «I servizi di accesso anonimo e i mezzi anonimi di pagamento sono la protezione migliore della privacy» (App. II, 3).

[65] Direttiva 1995/46/CE, art. 27.

[66] In base agli artt. 136 e 137 del codice della privacy, per i trattamenti effettuati: *a*) nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità; *b*) dai soggetti iscritti nell'elenco dei pubblicisti o nel registro dei praticanti di cui agli artt. 26 e 33 della legge 69/1963; *c*) in modo temporaneo e finalizzati esclusivamente alla pubblicazione o diffusione occasionale di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica, non sono richiesti: l'autorizzazione del Garante (prevista altrimenti dall'art. 26 del codice); il rispetto delle garanzie previste per i dati giudiziari (art. 27 del codice); l'osservanza degli accorgimenti previsti per i dati trasferiti all'estero (artt. da 42 a 45 del codice). Nei casi appena esposti il trattamento può essere effettuato anche senza il consenso dell'interessato previsto dagli artt. 23 e 26 del codice. In caso di diffusione o di comunicazione dei dati per le finalità di cui al citato art. 136 restano fermi i limiti del diritto di cronaca a tutela dei diritti di cui all'art. 2 e, in particolare, quello dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (su cui ci sofferma più diffusamente nel testo). Possono comunque essere trattati i dati personali relativi a circostanze o fatti resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico. Corte cost. [ord.], 5 marzo 2009, n. 66, in «Giust. pen.», 2009, I, 100, ha dichiarato manifestamente inammissibile la questione di costituzionalità – sollevata in riferimento all'art. 15 Cost. – dell'art. 137, comma 2, d.lgs. 196/2003, nella parte in cui non prevede il consenso dell'interessato al trattamento dei dati relativi alla corrispondenza epistolare che venga effettuato nell'ambito dell'attività giornalistica. Per altre fattispecie riconducibili al citato art. 137 si vedano: Cass. [ord.], sez. III, 24 aprile 2008, in «Riv. pen.», 2008, 880 (raccolta, da parte degli ideatori di un servizio televisivo, in assenza del consenso degli interessati e dell'autorizzazione del Garante, di campioni organici carpiti, con un comportamento ingannevole, ad alcuni deputati e senatori al fine di rinvenire eventuali tracce di sostanze stupefacenti: la Corte ha ribadito che il trattamento dei dati personali, pur attinenti a fatti di interesse pubblico in relazione al necessario profilo di essenzialità dell'informazione, non può prescindere dalla circostanza che detti fatti siano stati «resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico»; in argomento si veda anche Garante protezione dati personali, 10 ottobre 2006 e 19 ottobre 2006, in «Foro it.», 2007, III, 104 ss.); Trib. Avezzano, 29 marzo 2005, in «Dir. Internet», 2005, 463 (che ha ritenuto riconducibile all'art. 136, lett. *c*, la diffusione su un sito Internet della notizia relativa all'assunzione della qualità di indagato); Trib. Perugia, 31 maggio 2006, in «Danno e resp.», 2007, 689 (secondo cui la c.d. rilevanza sociale delle informazioni rilasciate durante un'intervista ne legittima la pubblicazione anche nell'ipotesi in cui queste debbano ritenersi riservate e confidenziali secondo la manifestazione di volontà dell'intervistato; al fine della qualificazione dell'evento lesivo della personalità dell'intervistato, l'esercizio del diritto di cronaca rende giuridicamente irrilevante anche la contrarietà del comportamento del giornalista al canone della correttezza professionale).

Il codice della privacy ha istituito un'autorità indipendente (denominata Garante per la protezione dei dati personali) al fine di assicurare un'efficace applicazione dei principi contenuti nel d.lgs. 196/2003. In particolare, i compiti sono elencati nell'art. 154. Al Garante l'art. 139 del codice della privacy (in linea con quanto statuito nell'art. 12 dello stesso d.lgs. 196/2003) ha anche affidato il compito di promuovere l'adozione, da parte del Consiglio nazionale dell'ordine dei giornalisti, di un apposito codice di deontologia relativo al trattamento dei dati personali effettuato nell'esercizio della professione di giornalista, contenente misure e accorgimenti a garanzia degli interessati rapportate alla natura dei dati, in particolare per quanto riguarda quelli idonei a rivelare lo stato di salute e la vita sessuale. Il codice in parola è stato adottato con provvedimento del Garante per la protezione dei dati personali del 29 luglio 1998 [Benedetti 1998].

C'è da chiedersi come mai una legge tanto dettagliata, per certi versi pedante, quando si è trattato di disciplinare il trattamento dei dati personali da parte dei giornalisti abbia rinunciato a dettare regole specifiche e rinviato il tutto all'emanazione di un codice di condotta elaborato dagli stessi interessati[67]. Eppure, le regole che disciplinano, ad esempio, il diritto di cronaca sono chiare [Melchionda e Pascuzzi 2005; Pascuzzi 2003b]. Il famoso «decalogo del giornalista» è stato canonizzato dalla Cassazione più di cinque lustri fa: la legge sulla privacy avrebbe quantomeno potuto riprodurre quei principi (e cioè che il diritto di cronaca è lecitamente esercitato se ricorrono l'utilità sociale dell'informazione; la verità oggettiva, o anche soltanto putativa; la forma civile dell'esposizione dei fatti)[68]. Invece il legislatore dice sostanzialmente ai giornalisti: «Datevi le regole e rispettatele».

Le risposte possono essere:

a) la delicatezza degli interessi in gioco. Stabilire i confini dell'esercizio del diritto di cronaca significa contemperare due posizioni di rilevanza costituzionale: la tutela della persona e la libertà di informazione. In tale contesto è difficile tracciare un confine netto: spesso tutelare la privacy significa individuare i confini con la tutela di altri interessi che con la stessa possono confliggere. Oltre a quanto detto a proposito della sicurezza dello Stato, si pensi ai seguenti possibili conflitti: privacy *vs.* libertà di stampa[69];

[67] Interpretando l'art. 8 del codice deontologico, che impone al giornalista di non fornire notizie o pubblicare immagini o fotografie di soggetti coinvolti in fatti di cronaca lesive della dignità della persona, ovvero di soffermarsi su dettagli di violenza, a meno che ravvisi la rilevanza sociale della notizia o dell'immagine, sempre fatta salva l'essenzialità dell'informazione, Cass., sez. trib., 31 marzo 2006, n. 7607, in «Dir. informazione e informatica», 2006, 342, ha chiarito che tale norma pone un divieto quando le notizie, le immagini o le fotografie dei soggetti coinvolti in un fatto di cronaca siano lesive della loro dignità e solo in via di deroga ne consente il superamento.

[68] Cfr. Cass., 18 ottobre 1984, n. 5259, in «Foro it.», 1984, I, c. 2711.

[69] L'art. 6 del codice deontologico dei giornalisti nel definire la nozione di «essenzialità dell'informazione» chiarisce che la divulgazione di notizie di rilevante interesse pubblico o sociale non contrasta con il rispetto della sfera privata quando l'informazione, anche dettagliata, sia indispensabile in ragione dell'originalità del fatto o della relativa descrizione dei modi particolari in cui è avvenuto, nonché della qualificazione dei protagonisti. La sfera privata delle persone note o che esercitano funzioni pubbliche deve essere rispettata se le notizie o i dati non hanno alcun rilievo sul loro ruolo o sulla loro vita pubblica. I commenti e le opinioni del giornalista appartengono alla libertà di informazione nonché alla libertà di parola e di pensiero costituzionalmente garantita a tutti. Per la casistica cfr. Cass., sez. I, 18 marzo 2008, n. 7261, in «Foro it.», 2008, I, c. 2159, che ha ritenuto lecita la pubblicazione su un quotidiano della fotografia di un imputato in stato di detenzione, ritratto in una posa in cui non erano visibili le manette, qualora la rivelazione dell'immagine sia effettuata per informare la cittadinanza su fatti delittuosi; App. Salerno, 15 settembre 2006, in «Foro it.», 2007, I, c. 594, che ha ritenuto illecita (in violazione del principio dell'essenzialità nell'informazione e delle regole sulla tutela dei minori coinvolti in fatti di cronaca) la pubblicazione su alcuni quotidiani delle generalità complete e della fotografia di un bambino di quattro anni deceduto a seguito del cedimento di un'acquasantiera all'interno di una chiesa.

privacy *vs.* prevenzione e repressione dei reati[70]; privacy *vs.* tutela della salute[71]; privacy *vs.* tutela dell'investitore[72]; privacy *vs.* trasparenza amministrativa[73];

b) la consapevolezza che norme rigide eteroimposte sono *tamquam non essent* nel momento in cui non vengono rispettate, e gli annali sono pieni di storie di mostri sbattuti in prima pagina, risultati successivamente del tutto estranei ai fatti loro addebitati (senza che questo si sia tradotto poi in qualche forma di responsabilità per i giornalisti, per non dire che una volta pubblicata la notizia il danno si è già verificato...);

c) l'idea che forse hanno maggiori possibilità di essere rispettate norme poste dagli stessi interessati, facendo leva non già sulla minaccia di una sanzione bensì sul senso di responsabilità di chi quelle regole è chiamato ad osservare e, di conseguenza, sulla capacità della stessa categoria di stigmatizzare i comportamenti non conformi al codice di autoregolamentazione.

Insomma, gli interessi in gioco sono delicati e qualsiasi intervento rigido del legislatore può intaccare ora l'una ora l'altra posizione costituzionalmente tutelata con il rischio di essere comunque inefficace. Meglio convincere

[70] Cfr. art. 15, direttiva 2002/58/CE.

[71] Come è noto la legge 5 giugno 1990, n. 135 (Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS) ha introdotto norme severe a tutela della riservatezza delle persone sieropositive. Ad esempio il comma 3 dell'art. 5 introduce il principio del divieto del c.d. *screening* obbligatorio di massa: per categorie a rischio di infezione HIV (consumatori di stupefacenti o omosessuali) o per categorie indesiderate (stranieri, immigrati). Ciononostante Corte cost., 2 giugno 1994, n. 218 («Foro it.», 1995, I, c. 46) ha dichiarato incostituzionale l'art. 5, comma 3, in parola nella parte in cui non prevede accertamenti sanitari dell'assenza di sieropositività all'infezione da HIV come condizione per l'espletamento di attività che comportino rischi per la salute di terzi. Sulla prevalenza del diritto alla salute sul diritto alla privacy nel caso si debba accedere a dati genetici indispensabili per la cura di una malattia cfr. Trib. minorenni Perugia, 4 dicembre 2001, in «Rass. giur. umbra», 2002, p. 417.

[72] Nella prestazione dei servizi di investimento, l'accesso da parte dell'intermediario alle informazioni relative alla situazione finanziaria e alla propensione al rischio del cliente costituisce per quest'ultimo una garanzia. Cfr. art. 21, comma 1, lett. *b*, del t.u. della finanza (d.lgs. 58/1998) nonché artt. 39 ss. del regolamento Consob 16190/2007.

[73] L'art. 24, comma 2, legge 7 agosto 1990, n. 241 mira ad operare un bilanciamento degli interessi che si collegano alla conoscenza dei documenti amministrativi, coordinandoli con gli interessi pubblici e privati legislativamente tutelati, che potrebbero essere ingiustamente lesi da quella conoscenza (riservatezza di terzi, persone, gruppi ed imprese, con garanzia peraltro per gli interessati della visione degli atti relativi ai procedimenti amministrativi, la cui conoscenza sia necessaria per curare o per difendere i loro interessi giuridici). Cfr. Cons. Stato, sez. VI, 19 giugno 2008, n. 3083, in «Foro amm.-Cons. Stato», 2008, 1826; Cons. Stato, sez. VI, 26 aprile 2005, n. 1896, in «Cons. Stato», 2005, I, 713; Cons. Stato, sez. V, 7 settembre 2004, n. 5873, in «Giur. it.», 2004, c. 2408.

quanti in concreto assicurano la libertà di informazione che è nel loro stesso interesse non compiere abusi, perché, ad esempio, una categoria che rispetti certe regole vede di per sé accresciuta la propria credibilità e difende nel modo migliore la propria libertà di manifestazione del pensiero. Di qui la scelta di dire ai giornalisti: «Datevi le regole e poi rispettatele».

Ragioni simili giustificano il ricorso a codici di condotta in un quadro più generale per salvaguardare la privacy nell'epoca di Internet. Anche in questo caso ci sono rilevanti interessi in gioco. E anche in questo caso è difficile l'*enforcement* di regole non spontaneamente sentite come vincolanti.

A tale proposito conviene ricordare che l'art. 12, d.lgs. 196/2003 attribuisce al Garante per la protezione dei dati personali il compito di promuovere, tenendo conto dei criteri stabiliti nelle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, la sottoscrizione di codici deontologici e di buona condotta per determinati settori[74]. In applicazione di tale disposizione il Garante ha fin qui promosso (oltre al già ricordato codice deontologico dei giornalisti) l'adozione dei seguenti provvedimenti: codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici[75]; codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del sistema statistico nazionale[76]; codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici[77]; codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti[78]; codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive[79].

Il d.lgs. 196/2003 prevede, inoltre, l'adozione di codici di deontologia e di buona condotta per il trattamento dei dati personali effettuati: *a*) per finalità previdenziali o per la gestione del rapporto di lavoro (art. 111); *b*) a fini di informazione commerciale (art. 118); *c*) con strumenti elettronici di rilevamento di immagini (art. 134); *d*) a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale (art. 140).

[74] Al Garante spetta anche il compito di verificare la conformità dei codici alle leggi e ai regolamenti, e di contribuire alla diffusione e al rispetto dei medesimi. I provvedimenti del Garante sono reperibili all'indirizzo http://www.garanteprivacy.it.

[75] Cfr. il provvedimento del Garante n. 8/P/2001 del 14 marzo 2001.

[76] Cfr. la deliberazione del Garante n. 13 del 31 luglio 2002.

[77] Cfr. il provvedimento del Garante n. 2 del 16 giugno 2004.

[78] Cfr. il provvedimento del Garante n. 8 del 16 novembre 2004.

[79] Cfr. il provvedimento del Garante n. 60 del 6 novembre 2008.

4.4. La tecnologia minaccia, la tecnologia protegge

La privacy degli individui viene minacciata dalle tecnologie. Ancora una volta la validità di tale affermazione non è circoscritta alla realtà contemporanea. Il *Domesday Book* (richiamato nell'Introduzione per sottolineare gli obiettivi che la tecnologia della carta ha consentito di raggiungere) conteneva una raccolta imponente di fatti su persone e proprietà[80]. L'elettronica ha solo amplificato i problemi in modo esponenziale tanto da rendere possibile forme invasive di sorveglianza sociale[81]. Nella risoluzione del Consiglio europeo del 22 marzo 2007 su una strategia per una società dell'informazione sicura in Europa, si legge (n. 4):

> già si sviluppano le nuove tecnologie che ci porteranno alla società dell'informazione onnipresente. L'avvento di tecnologie innovative (ad esempio reti senza filo ad alta velocità, dispositivi di identificazione a radiofrequenza (RFID), reti di sensori) e di servizi innovativi, ricchi di contenuti (ad esempio televisione su protocollo Internet (IPTV), *voice over IP* (VOIP), televisione mobile ed altri servizi mobili) richiede adeguati livelli di sicurezza delle reti e dell'informazione fin dall'inizio della fase di sviluppo per raggiungere reale valore commerciale.

[80] Lyon [1997] scrive: «Il *Domesday Book*, un registro delle proprietà terriere inglesi avviato nel 1086, conteneva una raccolta imponente di fatti su persone e proprietà. Questa cosiddetta *descriptio* permise all'amministrazione normanna, insediatasi con la forza delle armi, di consolidare il proprio potere [...] Era essenziale sapere, e stabilirlo nero su bianco, chi fosse tenuto a cosa».

[81] Eloquente sui possibili scenari preoccupanti è una frase pronunciata da Angela Bennet, protagonista del film *The Net*: «Ogni essere del mondo è inserito in un computer. È dentro il computer tutto quanto: i dati della sua targa, la sua previdenza sociale, le sue carte di credito, le sue malattie, le cure. È tutto registrato lì dentro. Ognuno è immagazzinato. C'è come una piccola ombra elettronica di ognuno di noi che aspetta solo di essere manipolata, contraffatta da qualcuno».

Sono tantissimi gli strumenti di uso quotidiano e di diffusione ormai capillare che favoriscono il monitoraggio della vita sociale: telecamere a circuito chiuso installate in luoghi pubblici e privati[82]; documenti di identità elettronici (carta di identità[83], carta nazionale dei servizi[84]; tessera sanitaria[85], tessera elettorale[86], passaporto contenente dati biometrici[87]); carte ma-

[82] Il Garante della privacy, in data 8 aprile 2010, ha emanato un provvedimento generale in materia di videosorveglianza che sostituisce quello del 29 aprile 2004. Precedentemente, il 29 novembre 2000, aveva emanato anche il decalogo per non violare la privacy nella stessa materia. Si vedano anche i provvedimenti del 4 settembre 2009 (Scuola: videosorveglianza contro atti vandalici); del 12 marzo 2009 (Prescrizioni per la videosorveglianza presso i siti di interesse culturale maggiormente esposti alla minaccia terroristica); del 26 febbraio 2009 (Prescrizioni per la videosorveglianza in un supermercato); del 19 febbraio 2009 (Videosorveglianza in un condominio); del 2 ottobre 2008 (Videosorveglianza: limiti e garanzie per il trattamento dei dati); dell'8 marzo 2007 (Videosorveglianza negli spogliatoi di una piscina). Si veda anche il d.p.r. 22 giugno 1999, n. 250, «Regolamento recante norme per l'autorizzazione all'installazione e all'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato». Trib. Milano 6 luglio 2007, in «Riv. critica dir. lav.», 2007, 1053 ha qualificato come comportamento antisindacale l'installazione di un sistema di videosorveglianza che (senza il preventivo accordo con le rappresentanze aziendali dei lavoratori o, in mancanza, l'autorizzazione della Direzione provinciale del lavoro) consenta il controllo a distanza sull'attività dei lavoratori. Per una fattispecie analoga cfr. App. Catania, 24 dicembre 2005, in «Mass. giur. lav.», 2006, 571. Della possibilità che l'installazione di una telecamera integri il reato di interferenze illecite nella vita privata si è occupata Cass. pen., sez. V, 21 ottobre 2008, in «Riv. pen.», 2009, 293, a cui dire il reato previsto dall'art. 615-*bis* c.p. non è configurabile per il solo fatto che si adoperino strumenti di osservazione e ripresa a distanza, quando tali strumenti siano finalizzati esclusivamente alla captazione di quanto avvenga in spazi che, pur se di pertinenza di una privata abitazione, siano però, di fatto, non protetti dalla vista degli estranei.

[83] Cfr. art. 66, d.lgs. 82/2005, codice dell'amministrazione digitale. L'art. 1, comma 1, lett. *c*, del codice (su cui cfr. più diffusamente il prossimo capitolo) definisce «carta d'identità elettronica» il documento d'identità munito di fotografia del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare.

[84] Cfr. art. 66, d.lgs. 82/2005. L'art. 1, comma 1, lett. *d*, del decreto definisce «carta nazionale dei servizi» il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni. Ai sensi dell'art. 64 dello stesso decreto la carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'autenticazione informatica. La carta d'identità elettronica e la carta nazionale dei servizi possono essere utilizzate quali strumenti di autenticazione telematica per l'effettuazione di pagamenti tra soggetti privati e pubbliche amministrazioni, secondo le modalità stabilite con specifiche regole tecniche (art. 66, comma 5).

[85] Cfr. art. 59, comma 50, lett. *i*, legge 449/1997; art. 2, d.l. 28 dicembre 1998, n. 450; art. 50, 269/2003. Per i profili di tutela della privacy, cfr. il Titolo V, d.lgs. 196/2003.

[86] Cfr. d.p.r. 8 settembre 2000, n. 299. L'art. 8 del decreto introduce la sperimentazione della tessera elettorale elettronica.

[87] Il regolamento del Consiglio europeo 2252/2004 (modificato da regolamento CE 444/2009) prevede il rilascio da parte degli Stati membri di passaporti e titoli di viaggio contenenti due elementi biometrici memorizzati su microchip: la fotografia e le impronte digitali del titolare. In argomento cfr. Corte giustizia Comunità europee, 18 dicembre 2007, n. 137/05, in «Raccolta», 2007, I, 11593.

gnetiche (carta di credito, *fidelity card*[88], telepass[89]); Tv interattiva[90]; servizi identificativi nella telefonia[91]; etichette elettroniche intelligenti[92]; e così via.

Anche le attività svolte su Internet possono essere facilmente spiate. Tra gli accorgimenti utili allo scopo (a parte *cookies* e *logs* di cui si è già parlato) si possono citare: i *web bugs* (o cimici web)[93]; gli *spywares* (codici in grado di raccogliere dati e inviarli al produttore del software in cui sono contenuti o a società che si occupano di telemarketing via Internet)[94]; gli *adwares* (*software advertising supported*)[95]; i dispositivi di *Digital rights management* (DRM)[96].

Ma se è vero che ritrovati tecnologici possono essere all'origine di intrusioni nella vita delle persone, è altrettanto vero che un uso accorto della tecnologia può scongiurare (o quanto meno depotenziare) i rischi più inquietanti.

Le c.d. *Privacy enhancing technologies* (PET) sono state sviluppate al fine di assicurare un grado sufficiente di riservatezza (se non di anonimato) nel cyberspazio. Con siffatta locuzione si suole individuare un sistema coe-

[88] La *fidelity card* consente all'azienda di conoscere i gusti del cliente. Su tale base, è possibile pianificare una strategia di marketing aggressiva diretta personalmente al singolo consumatore (*Customer relationship management*). Con provvedimento del 24 febbraio 2005 il Garante ha fissato le linee guida per un corretto utilizzo dei dati personali dei clienti da parte delle società che rilasciano le carte di fidelizzazione: informazione adeguata, libera scelta del consumatore, obbligo del consenso per profilazione e *direct marketing*.

[89] Il telepass, utilizzato per viaggiare in autostrada, registra: luogo, ora di entrata e uscita dai caselli, tempo di percorrenza e, confrontando i dati d'entrata e quelli d'uscita, la velocità media tenuta da casello a casello.

[90] Grazie ad apparecchi che combinano la tecnologia di Internet alla tv digitale, mentre il telespettatore guarda la televisione quest'ultima ne registra le abitudini.

[91] Sulla disciplina del servizio di identificazione del chiamante cfr. l'art. 125, d.lgs. 196/2003 e l'art. 8 della direttiva 2002/58/CE.

[92] Sull'argomento si tornerà nell'ultimo paragrafo di questo capitolo.

[93] Etichette elettroniche che aiutano siti web e imprese di pubblicità a seguire gli spostamenti dei visitatori sulla rete. Non più grandi di un *pixel*, spesso si nascondono all'interno di *banners* pubblicitari ed immagini. I *web bugs* sono presi in considerazione dal considerando n. 24 della direttiva 2002/58/CE.

[94] Oggetto della «raccolta» sono generalmente le informazioni relative a tipologie e licenze del software installato. Per i riferimenti normativi in Europa, cfr. art. 5 della direttiva 2002/58/CE e, in Italia, art. 122, d.lgs. 196/2003.

[95] Possono essere scaricati e utilizzati gratuitamente ma gli utilizzatori sono costretti a vedere *banners* pubblicitari a margine dell'applicazione. Gli *adwares* utilizzano la connessione ad Internet dell'utente per collegarsi periodicamente ai *servers* della compagnia di *advertising*. Durante il collegamento il software di *advertising* trasmette informazioni sull'utente e riceve nuovi *banners*: inutile dire che le compagnie di *advertising* sono in grado di inviare *banners* coerenti con il profilo che di sé l'utilizzatore ha fornito (ad esempio cliccando su un *banner* e quindi visitando il sito corrispondente).

[96] Con l'acronimo DRM si identificano le tecnologie di gestione (e controllo) dei contenuti digitali; per un'analisi approfondita di queste tematiche si rimanda al capitolo sul diritto d'autore.

rente di tecnologie dell'informazione e della comunicazione che proteggono la privacy eliminando o riducendo i dati personali o prevenendo un trattamento non necessario di dati personali senza compromettere la funzionalità del sistema. Le PET possono essere ricondotte a diverse tipologie:

– *subject-oriented PETs* (consentono di limitare la riconoscibilità di un determinato soggetto da parte di terzi)[97];

– *object-oriented PETs* (permettono di proteggere l'identità attraverso l'uso di tecnologie particolari)[98];

– *transaction-oriented PETs* (assicurano la protezione dei dati relativi alle transazioni, ad esempio perché li distruggono)[99];

– *system-oriented PETs* (creano zone di interazione dove l'identità dei soggetti è nascosta, gli oggetti non rilevano chi li ha trattati, i dati sulle transazioni non vengono mantenuti)[100].

Ci sono, infine, alcune PET che consentono ai navigatori della rete di programmare i propri *browsers* al fine di individuare le informazioni da rendere conoscibili ai titolari dei *web servers* mantenendo segreti invece i dati che non si vuole siano divulgati.

Tra le tecniche che possono essere usate a difesa della privacy devono essere ricordate, più in generale, la crittografia[101] e la steganografia[102].

[97] Un esempio di questo tipo di PET è rappresentato dagli *anonymizers*. Siti web (come Anonymizer.com) permettono la navigazione in forma anonima in quanto vengono bloccati *cookies*, Java, JavaScript e tutti gli altri sistemi di rilevamento presenti sulla rete. Vengono inoltre crittati i *cookies* e anche l'URL, in modo tale che nemmeno l'ISP possa tenere traccia della navigazione attraverso i *logs*. Un altro esempio è costituito dal *proxy server*, che permette di accedere ad un servizio (generalmente web) tenendo nascosto l'IP *address* dell'utente.

[98] È il caso del contante digitale di cui si parlerà nel capitolo dedicato alla moneta elettronica.

[99] Alcuni software si preoccupano di segnalare e rimuovere i *cookies* dall'*hard disk*. Uno di questi programmi si chiama *Real time cookie cleaner* e lavora con un utile sistema di «ingabbiamento» (*cookie jar*) dei *cookies*. Una lista aggiornata di questi programmi *shareware* è reperibile su http://www.tucows.com nella sezione dedicata ai *cookies* oppure su siti web che si occupano specificamente di protezione, come http://www.privacy.net.

[100] Gli *anonymous remailers* sono *servers* che permettono di inviare e-mail mantenendo l'anonimato. Detti *servers* si occupano di reinstradare la posta spedita eliminando ogni traccia del mittente. Alla stessa tipologia possono essere ricondotti i protocolli di riservatezza: SSL (*Secure socket layer*), S-HTTP (*Secure – Hypertext transfer protocol*), PCT (*Private communication technology*), SET (*Secure electronic transaction*).

[101] Tecnica che permette di «cifrare» un messaggio rendendolo incomprensibile a tutti fuorché al suo destinatario. In generale i due processi principali che vengono applicati in crittografia si dividono in «cifratura» e «codifica» (cfr. il capitolo dedicato alla firma digitale) [Giustozzi, Monti e Zimuel 2003; Ziccardi 2003].

[102] Insieme delle tecniche che consentono a due o più persone di comunicare tra loro in modo tale da nascondere, agli occhi di un eventuale osservatore, l'esistenza stessa della comunicazione. Il messaggio viene nascosto dentro un altro messaggio con diverso aspetto e contenuto, in modo che non sia possibile neppure rilevare l'esistenza stessa del messaggio segreto. Secondo una classificazione basata sull'origine del file «contenitore» (che può anche essere un'immagine) si può parlare di steganografia *iniettiva* e di steganografia *generativa*.

Il ricorso a meccanismi tecnologici come elemento di una strategia più globale di tutela della privacy viene incoraggiato anche sul piano normativo. Si veda quanto detto a proposito della sicurezza, muovendo dal considerando n. 46 della direttiva 1995/46/CE e dagli artt. 31 ss., d.lgs. 196/2003.

Va però sottolineato l'approccio molto radicale assunto dall'art. 3 del codice della privacy che ha canonizzato il principio di necessità nel trattamento dei dati:

> I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Se sistemi e programmi informatici devono essere configurati in modo da scongiurare essi stessi trattamenti incompatibili con i principi sanciti dalla legge, vuol dire che il legislatore affida alla stessa tecnologia il compito di assicurare il perseguimento degli obiettivi che le norme si prefiggono. In breve: la tecnologia incorpora la regola.

Una conferma di siffatto approccio si è avuta, di recente, nella raccomandazione della Commissione del 12 maggio 2009 sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza, su cui si tornerà più avanti. Il considerando n. 6 recita, infatti:

> Dato che la tecnologia RFID può essere utilizzata ovunque ed è praticamente invisibile, nell'adottarla particolare attenzione va tributata agli aspetti di protezione dei dati e della vita privata. Di conseguenza, prima di un loro uso generalizzato, le applicazioni RFID dovrebbero incorporare caratteristiche di tutela della sicurezza della vita privata e

delle informazioni (principio della «sicurezza e tutela della vita privata garantiti fin dalla fase di progettazione»).

4.5. Qualità e contrattualizzazione della tutela

Alla facilità con la quale Internet consente di raccogliere a costo pressoché nullo un numero rilevante di informazioni sugli individui, si accompagna la difficoltà di trovare meccanismi giuridici utili a tutelare in maniera effettiva la riservatezza sulla rete. Su un fenomeno conviene concentrare l'attenzione.

Molti siti web (in particolar modo quelli che vendono beni o forniscono servizi) enunciano in maniera esplicita la propria *privacy policy*, ovvero le regole che i gestori del sito si impegnano ad osservare in materia di trattamento dei dati personali dei navigatori. È sufficiente collegarsi al sito della Microsoft, o di Amazon, per trovare nella homepage (di regola in basso, ma comunque in evidenza) un *link* che conduce alle pagine nelle quali è appunto esplicitata la politica seguita in materia di privacy. Ma si tratta solo di esempi: come detto, sono molte migliaia i siti che attuano questo tipo di iniziativa. È utile cercare di comprendere le ragioni e la portata di questo fenomeno.

Data la stretta relazione tra tutela della privacy e decollo del commercio elettronico, i gestori dei siti si rendono conto che è loro stesso interesse rassicurare i potenziali clienti rendendo esplicite le politiche adottate in materia di dati personali.

Naturalmente enunciare alcune regole non significa garantire che le stesse vengano poi rispettate. Questo passaggio ulteriore è all'origine dei c.d. marchi a tutela della privacy. Uno degli strumenti utilizzati dalle aziende dell'industria *on-line* per garantire un effettivo *enforcement* della *privacy policy* è rappresentato dai *privacy seals*. Tali marchi nascono nell'ambito di iniziative di organizzazioni indipendenti con l'obiettivo di aumentare la fiducia dei consumatori nei confronti di Internet, per quanto riguarda lo specifico problema della riservatezza, al fine di accelerare la crescita dell'industria *on-line*. Il ruolo dei *privacy seal programs* è fondamentalmente quello di certificare, mediante apposizione di un marchio distintivo, che un determinato sito adotta pratiche sulla privacy conformi a quelle stabilite dal programma. Si tratta di marchi facilmente riconoscibili, la cui presenza avverte gli utenti che un certo sito ha raggiunto determinati standard di affidabilità per quanto riguarda la politica di tutela della privacy. Inutile dire che la presenza del marchio rappresenta un valore aggiunto per il sito web stesso[103].

Per quel che riguarda il nostro paese, il marchio di qualità *QWeb*, di cui si parlerà più diffusamente nel capitolo dedicato al commercio elettronico, attesta, tra l'altro, che il sito cui il marchio è rilasciato rispetta la normativa in materia di dati personali[104].

Alla luce di quanto esposto, la prassi della navigazione in Internet sembra sempre più uniformarsi al seguente paradigma.

Da un lato ci sono i siti web che danno notizia dei tipi di dati raccolti e dell'uso che ne verrà fatto; cercano il consenso per raccogliere quei dati; chiariscono in che modo viene garantita l'integrità e la sicurezza dei dati; chiariscono i rimedi disponibili nel caso la *privacy policy* non venga rispettata [Samuelson 2000]. Dall'altro c'è il navigatore che cerca nei siti beni e servizi.

La protezione della privacy risulta ancorata alla negoziazione (telematica) di un consenso al trattamento dei dati ottenuto a fronte dell'impegno a rispettare determinati principi in ordine al medesimo trattamento.

Il contenuto della tutela finisce con l'essere negoziato tra le parti. Chi pone le regole, di fatto, è il fornitore di beni e servizi, che oscilla fra la tentazione di utilizzare come vuole i dati raccolti e l'interesse a rispettare gli standard imposti da bollini di qualità se vuole mantenersi credibile.

Alla luce di quanto appena esposto, la prassi riscontrabile in Internet segna un significativo cambiamento di strategia nell'approccio alla tutela dei dati personali. L'atto normativo, di origine statale, ha rappresentato per molto tempo (specialmente in Europa) lo strumento utilizzato per discipli-

[103] Tra i principali programmi che attualmente gestiscono i *privacy seals* conviene ricordare: TRUSTe http://www.truste.com, BBB On-line http://www.bbbonline.org, CPA Webtrust http://www.webtrust.org. I *privacy seal programs* prevedono anche meccanismi semplificati per la risoluzione dei conflitti.

[104] Cfr. il punto 5, dell'allegato 1, della specifica *QWeb*, edizione 2.0, 1° gennaio 2005 (http://www.qwebmark.net/pdf/normativa_IT.pdf).

nare il trattamento computerizzato dei dati. Tale approccio ha alcune peculiarità: l'attribuzione ai soggetti di una posizione giuridica protetta in ordine ai dati che li riguardano; la fonte esterna della regola frutto della mediazione (politica) fra tutti gli interessi rappresentati nella società.

Il moltiplicarsi delle attività *on-line* fa intravedere un diverso modello di disciplina dei fenomeni in esame. La fonte diventa il contratto: la regola viene negoziata tra le parti in ragione dei loro esclusivi interessi nel momento in cui avviene l'incontro sulla rete. Si prescinde dalla preventiva allocazione di posizioni tutelate (che, in ipotesi, può anche non esistere).

4.6. Fascicoli sanitari elettronici e database genetici

Il codice della privacy dedica alcune disposizioni al trattamento dei dati sanitari (artt. 75 ss.) e dei dati genetici (art. 90). Conviene soffermarsi su un paio di problematiche che costituiscono altrettanti punti di frontiera del rapporto tra privacy e tecnologie informatiche: i fascicoli sanitari elettronici e i database genetici.

Il c.d. «Fascicolo sanitario elettronico» (FSE) rappresenta uno snodo cruciale nella digitalizzazione del trattamento dei dati sanitari. Esso consiste di due elementi fondamentali: il momento dell'archiviazione (attraverso strumenti digitalizzati) di tutti i dati e le informazioni che fino a quel momento erano state collazionate e gestite in modalità cartacea; il momento della condivisione dei dati così raccolti da parte di tutti gli attori del sistema, legittimati al loro trattamento e comunicazione.

Il Garante per la protezione dei dati personali, alla luce delle spinte all'implementazione di un sistema di FSE provenienti anche da documenti e raccomandazioni approvate in contesti sovranazionali[105], il 5 marzo 2009 ha varato un provvedimento a carattere generale avente ad oggetto le «Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario», avviando contestualmente una consultazione pubblica al fine di ricevere osservazioni e commenti, allo scopo di finalizzare questo momento di ascolto istituzionale degli *stakeholders* all'emanazione di un nuovo provvedimento contenente la cornice regolativa di riferimento per le future applicazioni di sanità elettronica in Italia. Il processo consultivo è culminato nell'emanazione, da parte dell'Autorità garante, di un provvedimento a carattere generale recante le «Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario – 16 luglio 2009»[106].

A queste indicazioni si è aggiunta, poi, una nuova presa di posizione del Garante, intervenuto con il provvedimento a carattere generale del 25 giugno 2009, recante «Linee guida in tema di referti *on-line*», che ha avviato un'altra consultazione pubblica al termine della quale il Garante ha, quindi, emanato le definitive «Linee guida in tema di referti *on-line* – 19 novembre 2009»[107].

L'avvento di una regolamentazione giuridica di dettaglio che interpreta l'esigenza di apprestare una tutela rinforzata per i dati sanitari oggetto di trattamento attraverso il FSE segna oggi un punto di svolta nel faticoso processo di sviluppo della sanità elettronica in Italia. Si tratta di un momento di cruciale importanza, perché dalla definizione giuridica di FSE discende l'ambito di applicazione di una serie di adempimenti e accorgimenti

[105] Cfr., ad esempio, il Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE), adottato il 15 febbraio 2007 dal Gruppo di lavoro sulla tutela dei dati personali istituito dall'art. 29 della direttiva 1995/46/CE.

[106] Le Linee guida definiscono FSE e *dossier* come insieme di dati sanitari relativi di regola ad un medesimo soggetto e riportati in più documenti elettronici tra loro collegati, condivisibili da soggetti sanitari diversi, pubblici e privati. Il FSE deve essere costituito preferendo, di regola, soluzioni che non prevedano una duplicazione in una nuova banca dati delle informazioni sanitarie formate dai professionisti o dagli organismi sanitari che hanno preso in cura l'interessato. In secondo luogo, provenendo i dati sanitari e i documenti riuniti nel FSE da più soggetti, devono essere adottate idonee cautele per ricostruire, anche in termini di responsabilità, chi ha raccolto e generato i dati e li ha resi disponibili nell'ambito del FSE. A garanzia dell'interessato, le finalità perseguite devono essere ricondotte solo alla prevenzione, diagnosi, cura e riabilitazione dell'interessato medesimo, con esclusione di ogni altra finalità (in particolare, per le attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, che possono essere, peraltro, espletate in vari casi anche senza la disponibilità di dati personali), ferme restando eventuali esigenze in ambito penale.

[107] I punti principali stabiliti dalle Linee guida sono i seguenti. L'adesione al servizio dovrà essere facoltativa e il referto elettronico non sostituirà quello cartaceo che rimarrà comunque disponibile. L'assistito dovrà dare il suo consenso sulla base di un'informativa chiara e trasparente che spieghi tutte le caratteristiche del servizio di refertazione *on-line*. Il referto resterà a disposizione *on-line* per un massimo di 45 giorni e dovrà essere accompagnato da un giudizio scritto e dalla disponibilità del medico a fornire ulteriori indicazioni su richiesta dell'interessato. Per fornire il servizio, le strutture sanitarie pubbliche e private dovranno adottare elevate misure di sicurezza tecnologica (utilizzo di standard crittografici, sistemi di autenticazione forte, convalida degli indirizzi e-mail con verifica *on-line*, uso di password per l'apertura del file) e, nel caso offrano la possibilità di archiviare e continuare a consultare via web i referti, dovranno anche sottoporre ai pazienti un'ulteriore specifica informativa e acquisire un autonomo consenso.

attraverso i quali i diritti del cittadino/paziente/interessato saranno tutelati, rendendo conforme a legalità il trattamento dei dati sanitari dei cittadini/pazienti operabile in via elettronica da una serie di soggetti (titolari), che sono accomunati dal fatto di essere investiti, nel momento del trattamento, dal compito di realizzare una finalità di cura rivolta a beneficio diretto del paziente/interessato a quei dati.

La definizione giuridica di FSE nel contesto regolativo della protezione dei dati personali non può che rispecchiare una visione della cura che il Sistema sanitario nazionale nel suo complesso (sistema nel quale prendono posto con ruoli e responsabilità differenziate, ma sempre più integrate, soggetti pubblici e privati) si ripromette di perseguire, nella consapevolezza che l'informazione assume, oggi più che mai, un ruolo chiave in qualsiasi processo riconducibile all'obiettivo ideale di tutelare la salute del cittadino/paziente/interessato [per maggiori approfondimenti si rinvia a Guarda 2010].

Un altro territorio di frontiera nel quale si manifesta oggi in modo particolarmente problematico il rapporto tra privacy e tecnologie informatiche è senz'altro rappresentato dal settore della ricerca biomedica[108]. Nell'ultimo decennio, in concomitanza con la mappatura dell'intero genoma umano[109], si è assistito, infatti, alla nascita di numerosi database genetici, ovvero grandi banche dati nelle quali sono conservati i profili genetici di centinaia di persone. Tali banche sono divenute strumenti irrinunciabili di indagine medica, visto che esse consentono di svolgere studi comparativi utili alla comprensione di numerose patologie nonché alla predisposizione di test diagnostici, di medicinali e principi attivi.

[108] In generale si deve ricordare che negli ultimi tempi ha preso il via un nuovo filone di studi denominato «bioinformatica». La bioinformatica può essere definita come la branca computazionale della biologia molecolare, oppure, osservandola da una diversa prospettiva, come la branca della scienza dell'informazione che si occupa della ricerca, dello sviluppo e dell'applicazione di strumenti computazionali in grado di facilitare l'acquisizione, l'archiviazione, l'organizzazione e l'analisi di dati biologici, medici, comportamentali o sanitari. La bioinformatica è dunque una scienza multidisciplinare che si pone a metà strada tra le scienze della vita e l'*Information technology*, impiegando i saperi derivanti dagli studi condotti nel settore informatico, statistico, matematico, chimico, fisico. Essa si presta ad essere impiegata in numerosi ambiti della biologia.

[109] La mappatura è avvenuta ed è stata condotta all'interno del progetto Genoma Umano, un progetto internazionale il cui scopo era la descrizione completa del genoma umano mediante il sequenziamento, cioè mediante l'identificazione della disposizione delle lettere del codice genetico, le basi nucleotidiche, lungo tutta la doppia elica del DNA. Nel progetto sono convogliati sia gli sforzi della ricerca pubblica di molte nazioni sia quelli di aziende private.

Fino a qualche decennio fa i tessuti biologici umani asportati durante le operazioni medico-chirurgiche erano destinati ad essere distrutti immediatamente dopo la raccolta con la conseguente perdita dei dati e delle informazioni in essi contenuti, oppure, nella migliore delle ipotesi, potevano essere utilizzati dal sanitario o dall'équipe medica che ne aveva curato la raccolta a fini di ricerca medica, il più delle volte senza il consenso del paziente.

L'impiego di tali campioni biologici avveniva dunque a scapito sia dei pazienti, i quali non avevano alcuna possibilità di controllare l'utilizzo dei loro campioni, sia della scienza medica. L'uso domestico dei campioni biologici precludeva, infatti, la possibilità di condividere in rete tali campioni, per renderli di volta in volta accessibili a quei ricercatori che ne avessero avuto la necessità per studiare una determinata patologia. In tale contesto, ogni ricercatore poteva accedere ai soli campioni biologici dei pazienti che aveva in cura o comunque a un bacino di casi clinici limitato. Ciò costituiva un ostacolo alle possibilità della ricerca, specie per lo studio di quelle malattie definite rare che possono essere meglio combattute muovendo dall'osservazione di pool di casi più vasto.

I database genetici hanno rappresentato un punto di svolta rispetto al panorama fin qui descritto. In primo luogo, la catalogazione sistematica dei profili genetici ottenuti dai campioni biologici facilita l'accesso da parte dei ricercatori ai dati. Inoltre, tali database aggregano una quantità di informazioni considerevolmente maggiore rispetto al passato, consentendo di porre in essere studi comparativi. In terzo luogo, i database possono essere inseriti in un sistema di reti, che permette la condivisione delle informazioni a livello globale.

A questo proposito, non è affatto peregrino intravedere un'analogia tra i database genetici e le biblioteche, dato che la catalogazione del DNA ottenuto dai tessuti promette di produrre per la ricerca scientifica lo stesso effetto rivoluzionario che le biblioteche hanno comportato per la conoscenza dell'umanità a seguito della comparsa del libro. I profili genetici, al pari dei libri, contengono informazioni, benché particolari [Macilotti 2008]. Essi, infatti, racchiudono la storia biologica del soggetto al quale il profilo genetico si riferisce e, in parte, la storia biologica della sua famiglia. Come l'organizzazione e la catalogazione nelle biblioteche ha permesso ai libri di essere prima conosciuti e poi diffusi presso il grande pubblico, così i bio-database

consentono di agevolare l'accesso e l'utilizzo delle informazioni in essi contenuti al mondo della ricerca. Per poter essere fruibile il sapere deve essere organizzato e i database genetici rispondono a questa funzione.

Accanto all'indubbio valore scientifico assunto dai database genetici, vi è da registrare come, sul versante giuridico, questi strumenti abbiano generato profonde preoccupazioni, soprattutto con riguardo alla tutela della riservatezza delle persone coinvolte. Tali preoccupazioni sono sorte in ragione del fatto che i database custodiscono i dati genetici di una grande quantità di individui, dati che appartengono alla categoria di dati sensibili, visto che sono in grado di rivelare lo stato di salute del soggetto al quale si riferiscono, non soltanto in riferimento al presente, ma anche in chiave di predittività futura. Inoltre, in quanto ereditati, essi hanno la peculiarità di non riguardare soltanto l'individuo ma anche il suo gruppo biologico. Chi gestisce e controlla l'accesso ai database genetici controlla dunque l'identità biologica di migliaia di individui.

La vicenda che ha portato alla ribalta il dibattito etico e giuridico sui database genetici, evidenziandone le criticità, è senza dubbio rinvenibile nell'approvazione (avvenuta nel 1998) da parte del Parlamento islandese dell'*Act on a Health Sector Database* che ha autorizzato la creazione dell'*Health Sector Database* (HSD), una grande banca dati che raccoglie dati medici e genetici contenuti in tutte le banche dati locali già presenti nel sistema sanitario nazionale islandese.

La novità della norma approvata dal Parlamento islandese risiede non solo nell'aver creato una banca dati genetica della popolazione, ma nell'aver concesso il diritto esclusivo di raccolta e di stoccaggio del patrimonio genetico dell'intera popolazione a una società privata alla quale è stato conferito il diritto esclusivo di sfruttare i dati e i benefici economici da essi derivanti. Grazie a questa legge, le singole banche dati periferiche, amministrate dal sistema sanitario nazionale, sono state connesse in un grande database elettronico, creato e gestito da una società privata, la quale ha ottenuto il diritto di sfruttamento esclusivo di tali banche da parte del governo islandese.

Le preoccupazioni seguite a questa vicenda hanno spinto i legislatori nazionali ad emanare norme particolarmente restrittive con riguardo alla costituzione e alla gestione di tale tipologia di database. Nel nostro paese il codice della privacy prevede una peculiare tutela per il trattamento dei

dati genetici, subordinandolo, secondo quanto previsto dall'art. 90, all'emanazione di apposite autorizzazioni del Garante per la protezione dei dati personali. Ad oggi, l'unica autorizzazione emanata dal Garante risale al 22 febbraio 2007 e, sebbene sia in attesa di rinnovo, è ancora operante.

Con riguardo ai database genetici, l'autorizzazione prevede che i dati genetici e i campioni biologici contenuti in elenchi, registri o banche di dati debbano essere trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità, in modo da ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato. Laddove gli elenchi, i registri o le banche di dati contengano anche dati riguardanti la genealogia o lo stato di salute degli interessati, le predette tecniche devono consentire, altresì, il trattamento disgiunto dei dati genetici e sanitari dagli altri dati personali che permettono di identificare direttamente le persone interessate. L'autorizzazione prevede dunque l'adozione di misure tecniche di sicurezza particolarmente pesanti, così da ridurre al minimo il rischio per i soggetti di un utilizzo distorto dei loro dati. Tuttavia la gestione di tali database rimane una questione particolarmente delicata, soprattutto se, pur senza abbracciare logiche riduzionistiche, si considera che il loro contenuto informazionale è destinato ad aumentare sensibilmente con la conoscenza del genoma umano [per ulteriori approfondimenti si rinvia a Macilotti 2008; 2009; Macilotti *et al.* 2008].

4.7. Privacy e Internet degli oggetti. In particolare: le tecnologie RFID

Nell'Introduzione si è fatto riferimento allo scenario che si sta schiudendo rappresentato dalla possibilità di interconnettere non solo i computer ma anche oggetti. Questa realtà, cui è stato dato il nome di «Internet degli oggetti», fa assegnamento su tecnologie come l'identificazione a radiofrequenza. Inutile dire che, ancora una volta, gli indubbi vantaggi derivanti da questi ritrovati si accompagnano a nuove minacce per la privacy delle persone.

La Commissione europea ha emanato, in data 12 maggio 2009, una

raccomandazione[110] sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza (2009/387/CE). Il documento definisce «identificazione a radiofrequenza» (RFID) l'uso di onde elettromagnetiche o l'accoppiamento di un campo reattivo nella porzione di radiofrequenza dello spettro per comunicare a partire da o verso un'etichetta mediante una varietà di sistemi di modulazione e codifica allo scopo di leggere, in modo univoco, l'identità di un'etichetta di radiofrequenza o altri dati in essa registrati.

L'identificazione a radiofrequenza si sta progressivamente diffondendo e sta entrando a far parte della vita quotidiana dei singoli in una serie di ambiti, quali la logistica, la sanità, i trasporti pubblici, il commercio al dettaglio (al fine di migliorare la sicurezza e accelerare il richiamo dei prodotti), i divertimenti, il lavoro, la gestione dei pedaggi stradali, dei bagagli e dei documenti di viaggio. La tecnologia RFID ha le potenzialità per divenire un nuovo catalizzatore della crescita e dell'occupazione, trattandosi di un ambito estremamente promettente in termini economici che può consentire nuove opportunità imprenditoriali, riduzioni dei costi e aumento dell'efficienza, soprattutto per quanto riguarda la lotta alla contraffazione, la gestione dei rifiuti elettronici (*e-waste*), dei materiali pericolosi e dei prodotti alla fine del ciclo di vita (cfr. i considerando nn. 2 e 3 della raccomandazione).

Sempre sul piano terminologico «etichetta RFID» o «etichetta» è un dispositivo RFID in grado di produrre un segnale radio o un dispositivo RFID che riaccoppia, retrodiffonde o riflette (a seconda del tipo di dispositivo) e modula un segnale portante ricevuto da un apparecchio di lettura o di scrittura.

Un «apparecchio di lettura o apparecchio di scrittura RFID» è un dispositivo fisso o mobile per la cattura e l'identificazione di dati utilizzando un'onda elettromagnetica a radiofrequenza o l'accoppiamento di un campo reattivo per stimolare ed eseguire una risposta modulata di dati da un'etichetta o gruppo di etichette.

Le applicazioni RFID consentono potenzialmente l'elaborazione di dati relativi a una persona fisica identificata o identificabile, direttamente o indirettamente. In particolare tali applicazioni permettono di elaborare i dati

[110] Notificata con il numero C(2009) 3200.

personali contenuti sull'etichetta, quali il nome, la data di nascita o l'indirizzo di una persona o i dati biometrici o ancora i dati che collegano il numero di un elemento RFID specifico a dati personali stoccati altrove nel sistema. Tale tecnologia, inoltre, potrebbe essere utilizzata per controllare singole persone che sono in possesso di uno o più elementi contenenti il numero di un elemento RFID (cfr. il considerando n. 5 della raccomandazione).

La raccomandazione prende in considerazione i seguenti profili: la valutazione dell'impatto sulla protezione della vita privata e dei dati stessi; la sicurezza delle informazioni; le informazioni e la trasparenza sull'uso della RFID; l'utilizzo della RFID nel commercio al dettaglio; l'attività di sensibilizzazione; l'attività di ricerca e sviluppo.

Per quel che riguarda, specificamente, l'impatto sulla protezione della vita privata e dei dati, secondo la raccomandazione, gli Stati membri dovrebbero garantire, tra l'altro, che (fatti salvi i loro obblighi in virtù della direttiva 1995/46/CE) gli operatori:

a) eseguano una valutazione delle implicazioni che l'introduzione delle applicazioni in esame ha per la protezione dei dati personali e della vita privata, verificando se tali applicazioni possano essere utilizzate per controllare singole persone;

b) adottino le misure tecniche e organizzative adeguate per garantire la protezione dei dati personali e della vita privata;

c) designino una persona o un gruppo di persone cui affidare la revisione delle valutazioni e la verifica della costante adeguatezza delle misure tecniche e organizzative adottate per garantire la protezione dei dati personali e della vita privata;

d) mettano la valutazione a disposizione delle autorità competenti almeno sei settimane prima di introdurre l'applicazione;

e) attuino le disposizioni di cui sopra conformemente al quadro per le valutazioni d'impatto sulla protezione dei dati e la tutela della vita privata che gli stessi Stati membri sono chiamati ad elaborare.

Per quel che riguarda, invece, le informazioni e la trasparenza sull'uso della RFID, secondo la raccomandazione gli Stati membri dovrebbero garantire che i gestori elaborino e diffondano una politica informativa concisa, accurata e di facile comprensione per ciascuna delle loro applicazioni, che comprenda quantomeno:

a) l'identità e l'indirizzo dei gestori;

b) le finalità dell'applicazione;

c) i dati elaborati dall'applicazione, specificando in particolare se saranno elaborati dati personali e se sarà controllata l'ubicazione delle etichette;

d) una sintesi della valutazione d'impatto sulla tutela della vita privata e la protezione dei dati;

e) gli eventuali rischi per la vita privata relativi all'uso delle etichette nell'applicazione e le misure che i singoli possono adottare per ridurre tali rischi. Gli Stati membri dovrebbero anche accertarsi che i gestori adottino misure per informare i singoli della presenza di lettori utilizzando un simbolo europeo comune messo a punto dagli organismi europei di normalizzazione con il sostegno delle parti interessate. Il simbolo dovrebbe indicare l'identità del gestore e un punto di contatto cui i singoli possano rivolgersi per procurarsi la politica informativa relativa all'applicazione.

Sul tema è intervenuta la direttiva 2009/136/CE il cui considerando n. 56 recita, tra l'altro:

> Quando tali dispositivi (RFID) sono collegati a reti di comunicazione elettronica accessibili al pubblico, o usano servizi di comunicazione elettronica come infrastruttura di base, è opportuno che si applichino le disposizioni pertinenti della direttiva 2002/58/CE (vita privata e comunicazioni elettroniche), in particolare quelle sulla sicurezza, sui dati relativi al traffico e alla localizzazione e sulla riservatezza.

(Di Internet degli oggetti si tornerà a parlare nel capitolo dedicato alla destatualizzazione contenuto nella seconda parte del volume).

In sintesi: dall'analisi svolta in questo primo capitolo dedicato ai diritti della personalità, la premessa da cui si sono prese le mosse (connessione tra diritto e tecnologia) riceve le prime conferme. Si può dire, infatti, che, per quanto attiene alla tutela della riservatezza, l'avvento dell'era digitale comporta i seguenti cambiamenti sul piano delle regole giuridiche:

– il contenuto del diritto alla riservatezza si trasforma e si amplia: dal diritto ad essere lasciati soli al diritto al controllo sulle informazioni che riguardano l'individuo, fino a giungere all'enunciazione del diritto alla protezione dei dati personali;

– (più specificamente dopo l'esplosione di Internet) si diversificano le ragioni per tutelare la privacy: il problema non è più tanto (o non solo) evitare discriminazioni, quanto tranquillizzare i potenziali clienti del commercio elettronico;

– le regole tradizionali (di provenienza statuale e destinate ad operare in ambiti spaziali definiti) si mostrano inidonee a governare il carattere aterritoriale della rete e ad assicurare l'*enforcement* dei precetti normativi;

– si affermano approcci alternativi per disciplinare il trattamento dei dati personali. Tra questi: i codici deontologici e di condotta, le tecnologie che proteggono l'anonimato, la certificazione di qualità, la negoziazione diretta tra le parti;

– si tende ad affidare alla stessa tecnologia il rispetto delle norme sul trattamento dei dati personali, e si chiede alla tecnologia di incorporare la regola.