PUBBLICAZIONE QUADRIMESTRALE
ANNO XXI - N. 2 MAGGIO - AGOSTO 2005

ISSN 1123-5055

comma 20/b, art. 2 - Legge n. 662/96 - Fil. di Padova

Contratto e impresa

Dialoghi con la giurisprudenza civile e commerciale
diretti da Francesco Galgano

2

ventunesimo anno

Il governo del contratto: il riequilibrio delle prestazioni; la rinegoziazione del contratto di durata; la ragionevolezza; la giustizia del contratto; i nuovi sviluppi giurisprudenziali sulla buona fede contrattuale

Riforma del diritto societario: controllo giudiziario sull'amministrazione; fusione e trasformazione di società; azione di responsabilità contro gli amministratori

Informatica: la firma digitale; *internet* fra tecnica e diritto

Disponibilità del diritto all'immagine

Bond Argentina e validità del contratto di investimento; la riforma della Banca d'Italia

2005

CEDAM - PADOVA

INFORMATICA

ALESSANDRO MANTELERO

Regole tecniche e regole giuridiche: interazioni e sinergie nella disciplina di *internet* (*)

SOMMARIO: 1. Struttura informatica e limiti alla regolamentazione di *internet*. - 2. Alla ricerca di una tecnologia «conformata». - 3. Regole tecniche e *digital privacy*. - 4. Verso una sinergia fra diritto e tecnologia.

1. - È ormai fuor di dubbio che il computer prima ed *internet* in seguito abbiano concorso ad una svolta epocale nella società moderna sotto il profilo comunicativo, relazionale, comportamentale e commerciale (1). Tale cambiamento ha inciso sulla realtà che le norme giuridiche erano tradizionalmente chiamate a regolare, in termini di capacità di identificazione dei soggetti con cui ci si rapporta, di quantità di informazioni personali disponibili, di controllo sulle manifestazioni del pensiero e da ultimo, ma non certo con minor importanza, di modalità di conclusione dei rapporti negoziali.

A fronte di questi mutamenti non pare oggettivamente possibile negare che già solo con riguardo alla normalità dell'agire comune (comunicare, porsi in relazione con gli altri, contrarre) occorra una riflessione sulle norme applicabili ad *internet*. In merito non sembrano convincenti le soluzioni «estreme» al problema: né l'approccio che potremmo definire «conservatore», secondo cui le disposizioni vigenti sono sufficienti alla

(*) Il presente contribuito, ad eccezione delle note, costituisce il testo della relazione tenuta al convegno *Digital Privacy: un dialogo a più voci*, svoltosi il 18-19 aprile 2005 presso la Facoltà di giurisprudenza dell'Università di Torino, i cui atti sono in corso di pubblicazione.

(1) Cfr. a riguardo: DE ROSA, *La formazione di regole giuridiche per il "cyberspazio"*, in *Dir. informaz. e informat.*, 2003, p. 364; VITERBO-CODIGNOLA, *La rete tecnologia di libertà?*, *ivi*, 2003, p. 219 ss. ed ID., *L'informazione e l'informatica nella società della conoscenza*, *ivi*, 2002, p. 31 ss.; DE RITA, *Progressi tecnologici dell'informazione e società*, Roma, 13 gennaio 1996, intervista pubblicata su *www.mediamente.rai.it* (visitato il 24 aprile 2005).

regolamentazione del mutato contesto, a cui vanno applicate facendo per lo più ricorso all'analogia, né quello «innovativo» che auspica l'avvento di un non meglio definito *cyberlaw*, sulla cui opportunità ci si può interrogare e di cui non paiono ancor oggi chiari i confini (2).

Appare infatti tanto errato negare l'evidenza dei mutamenti connessi alla diffusione di *internet*, quanto semplicistico teorizzare l'esistenza di un *cyberspazio* costituente una realtà parallela quasi simile a quella generata dall'immaginazione letteraria di William Gibson (3).

Da questi cenni emerge dunque come la valutazione delle scelte attinenti le modalità con cui addivenire ad una regolamentazione di *internet*, e conseguentemente alla definizione dei confini della *digital privacy*, implichino necessariamente una preventiva qualificazione dell'oggetto dell'eventuale disciplina, definendone la natura.

In tal senso, negato il carattere spaziale di «luogo» alla realtà di *internet*, e quindi ogni valore - se non meramente simbolico - all'abusata contrapposizione fra «reale» e «virtuale», si deve concludere che si è di fronte non ad un nuovo mondo (4), ma ad un nuovo mezzo di comunicazione (5). Così come una conversazione telefonica non crea una realtà paral-

---

(2) Si rinvia alle considerazioni critiche più ampiamente espresse in MANTELERO, *Attività di impresa in Internet e tutela della persona*, Padova, 2004, p. 9 ss.

(3) Cfr. GIBSON, *Neuromancer*, New York, 1984. L'a., considerato il caposcuola del *cyberpunk*, tendenza letteraria nata alla fine degli anni Settanta del secolo scorso, così definisce il *cyberspazio* nel suo romanzo: «reticoli luminosi di logica dispiegata attraverso... vuoto incolore» costituito di banche dati strutturate secondo modelli geometrici, a cui si accede mediante connessioni dirette al cervello, attraverso elettrodi che consentono la visione di quella che è definita «la matrice». In generale sulla letteratura *cyberpunk* cfr. GATTO, *Cyberpunk*, Torino, 2002, p. 3 ss., in cui si definisce il *cyberpunk* come «un genere narrativo nato da un gruppo di *hacker* strafatti, professionisti invasati del *computer*, scrittori allucinati e superstiti della cultura *West Coast*. CP [*cyberpunk*] ha letteralmente inventato un modo diverso di guardare al reale e ha dovuto inventare un linguaggio - informatico, contaminato, febbrile, indefinito ma spaventosamente preciso - per raccontare la realtà virtuale, le personalità condivise (scisse, separate, frammentate, incoerenti), il mondo dei marchi e degli imperi di dati e di flussi di informazione»; in specie si segnalano le antologie *Mirrorshades*, a cura di B. Sterling, Milano, 1994 e *Cyberpunk*, a cura di P. Nicolazzini, Milano, 1994.

(4) Cfr. invece IRTI, *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari, 2002, p. 66, il quale afferma: «lo spazio telematico si stende sopra la terra come un sopra-mondo, un'epidermide, popolata di esseri intangibili, percepiti soltanto dal nostro occhio e dal nostro orecchio. Il 'navigante' non si sposta da un luogo all'altro, non lascia una terra per un'altra, ma si muove in un indefinito campo di energia».

(5) Cfr. G. FINOCCHIARO, *Lex mercatoria e commercio elettronico. Il diritto applicabile ai contratti conclusi su Internet*, in *questa rivista*, 2001, p. 571 ed ora in *Diritto di internet. Scritti e materiali per il corso*, Bologna, 2001, p. 1, secondo cui *internet* «non è un luogo ma è un

lela semplicemente per il fatto di sminuire l'aspetto fisico correlato alla compresenza dei soggetti, analogamente la comunicazione attraverso *internet*, sebbene arricchita da contenuti multimediali, permane in un contesto reale costituito da *bit*, reti, *router* (6), *server* e terminali. La visione di uno spazio parallelo è quindi semplicemente l'effetto di una percezione incompleta del mezzo.

La negazione dell'esistenza di una realtà separata non risolve tuttavia i problemi giuridici che proprio tale semplificazione immaginifica mette in luce, sintetizzando, seppure in maniera errata, la peculiarità della comunicazione che si realizza attraverso questo nuovo mezzo. I caratteri con cui detta comunicazione si svolge sono conseguenza immediata della struttura stessa secondo cui si è sviluppata *internet*, è dunque da questo livello più profondo che l'analisi deve iniziare.

Almeno quattro paiono le connotazioni che contraddistinguono la rete: diffusività, accessibilità, interoperatività, flessibilità.

Con riguardo al primo profilo è evidente come la presenza capillare delle strutture di rete in tutto il mondo industrializzato (7) renda in linea di

---

mezzo di comunicazione: ed è, per di più, un mezzo di comunicazione che per sua natura rende assai difficoltosa la collocazione geografica dei soggetti che di esso si servono per comunicare». Osserva invece IRTI, *op. cit.*, p. 66: «il *computer* non è un mezzo per stare nel mondo. Il mezzo ha creato il proprio mondo, nel quale si può entrare o non entrare».

(6) I *router* (in inglese letteralmente *instradatore*) sono dispositivi informatici in grado di collegare fra loro più reti in maniera tale da indirizzare i pacchetti di dati secondo il percorso più rapido, con gestione dei protocolli di trasmissione (per la definizione di «protocollo di trasmissione» cfr. *infra* nota 45). Tali dispositivi possono consistere in normali *computer* dotati di un apposito *software* o, più spesso, apparati specializzati dedicati a questo solo scopo. Cfr. voce *Router*, in *Wikipedia, l'enciclopedia libera*, disponibile al sito *www.it.wikipedia.org*.

(7) Va in proposito osservato come comunemente si affermi la natura «globale» di *internet*, rappresentando tale rete informatica come diffusa sull'intero orbe terraqueo. Tale impostazione risente significativamente di una visione parziale della realtà, caratterizzata da un'evidente tendenza autoreferenziale propria di chi appartiene al mondo industrializzato, dimenticando che ad oggi la quasi totalità delle risorse di rete è localizzata nel Nord America e nell'Unione Europea (che con il 19% della popolazione generano l'80% dell'attività in rete), oltre che in Giappone ed Australia. Gran parte del mondo pare infatti esclusa dall'accesso ad *internet* (e purtroppo a ben più essenziali risorse!). Difficile è addivenire ad un'esatta quantificazione degli utenti connessi ad *internet*, nonché definire la loro distribuzione per aree geografiche. Su tali stime incidono infatti in maniera distorsiva almeno tre fattori: la diversità dei parametri statistici adottati nelle differenti rilevazioni nazionali, la varietà delle metodologie di indagine impiegate, il margine di errore intrinsecamente connaturato al rilevamento a campione. Per tali ragioni può essere utile ricorrere a metodologie di stima incentrate su dati tecnici correlati alla struttura della rete stessa, come accade

principio possibile la fruizione dei contenuti veicolati da tale mezzo di comunicazione in maniera globale e contemporanea da parte di chiunque sia connesso. Già in tale aspetto possiamo quindi rilevare una dimensione dell'accessibilità della rete, tuttavia questa seconda aggettivazione tende a sottolineare specialmente l'assenza di barriere, se non di condizioni economiche, per chi desideri divenire parte della rete a diversi livelli. *Internet*, dopo la fase iniziale ([8]), si è infatti sviluppata secondo una struttura non proprietaria ([9]), per cui non esiste un unico soggetto a cui fanno capo tut-

---

ricorrendo al cd. *hostcount*: gli *host* (corrispondenti ad indirizzi IP permanenti ed attivi) rappresentano infatti punti fissi dell'architettura di *internet* di più agevole ricognizione e capaci di rivelare implicitamente la diffusione della rete. Sebbene non vi sia un collegamento diretto fra numero di utenti e numero di *host*, mediante il conteggio di quest'ultimi è possibile monitorare l'attività di utilizzo della rete; va in proposito precisato che in tale rilevazione la nazionalità dell'*host* è determinata in ragione del luogo di registrazione del nome a dominio, il che comporta la necessità di correggere il margine di errore che così si viene a creare ogniqualvolta un *host* venga registrato sotto il TLD nazionale di uno stato diverso da quello ove risiede fisicamente il proprio *server*. Seguendo tale metodo d'analisi, sulla base dell'elaborazione dei dati aggiornati al dicembre 2004, mentre la media europea di *host* ogni 1000 abitanti è pari ad 82, si scende a 16 con riguardo all'America latina, ad 8 per il continente asiatico e solamente a 0,8 per l'Africa, con un rapporto rispettivamente pari ad un quinto, un decimo e un centesimo del livello europeo. Paiono dunque più che fondate le osservazioni espresse nell'ultimo rapporto sulla diffusione di *internet* disponibile sul sito *www.gandalf.it* (visitato il 23 aprile 2005), secondo cui: «il quadro generale è sempre lo stesso. La 'globalità' dell'*internet* è limitata a una piccola parte del globo. L'uso della rete rimane concentrato sulle due sponde dell'Atlantico settentrionale e in punti isolati dell'Oceania, dell'Asia Orientale e del Medio Oriente. C'è un'evoluzione veloce in alcuni paesi dell'America Latina - anche se ancora lontana dai livelli degli Stati Uniti, del Canada e dell'Europa. Il resto del mondo è quasi completamente escluso». I dati qui riportati sono stati tratti dal sito *www.gandalf.it* e derivano da elaborazioni delle statistiche pubblicate da *Network Wizards* (cfr. il sito *web www.nw.com*), riferite a dati aggiornati al dicembre 2004.

([8]) Il nucleo iniziale di *internet* era costituito dalla rete *Arpanet* creata negli Stati Uniti a partire dal 1969 dall'agenzia del Pentagono denominata ARPA (*Advanced Research Projects Agency*): la realizzazione di tale rete era finalizzata a mettere in collegamento diversi elaboratori utilizzati dai ricercatori informatici del governo. Nel 1973 la rete era composta di venticinque *computer* connessi tra loro attraverso una struttura decentrata e non gerarchizzata. In seguito questa rete informatica è stata ampliata ed utilizzata per scopi civili, consentendo a chiunque di connettersi. Molto più tardi, nel 1993, con la creazione del *World Wide Web*, ossia un sistema in grado di legare fra loro una molteplicità di documenti attraverso vari rimandi intertestuali, si è poi avuto un ulteriore consistente miglioramento del funzionamento di *internet*, che ne ha consentito la rapida diffusione su grande scala.

([9]) Le uniche parti della struttura maggiormente controllabili sono le reti impiegate per la trasmissione dei dati (telefoniche, a fibre ottiche, ecc.), tuttavia non c'è interesse da parte dei proprietari delle stesse a limitare la crescita di *internet*, anzi la sua diffusione della

te le risorse che la compongono ([10]), come accade nelle reti *intranet* ([11]). Pur permanendo una proprietà esclusiva di ciascuno sui mezzi dallo stesso impiegati nel contribuire alla costruzione di *internet* (terminali, *server* ([12]), *router*, reti di comunicazione), la rete in sé costituisce un aggregato capace di funzionare anche in assenza dell'apporto di una parte ed in grado di rimodellarsi creando nuovi collegamenti ([13]), non essendo concepita secondo un modello piramidale ([14]). In tal contesto chiunque può do-

---

stessa ha costituito una fonte di rilancio per i tradizionali servizi di comunicazione via cavo e di sviluppo per gli innovativi sistemi *wi-fi*.

([10]) Cfr. G. FINOCCHIARO, *Lex mercatoria e commercio elettronico. Il diritto applicabile ai contratti conclusi su Internet*, cit., p. 571 ss.

([11]) Viene così denominata una rete di *computer* non collegata con l'esterno, generalmente costituita da un'impresa o da un privato al fine di favorire la circolazione dei dati fra i diversi elaboratori utilizzati per la propria attività.

([12]) Il *server* è un *computer* connesso alla rete che raccoglie centralmente informazioni ed elabora risorse, con funzioni specifiche che vanno dalla gestione di posta elettronica o di pagine *web* alla fornitura di servizi di connessione di vario genere.

([13]) I collegamenti fra i diversi nodi di rete sono infatti incentrati su criteri statistici di disponibilità e non su criteri totalmente deterministici propri di diverse applicazioni informatiche. Cfr. voce *Internet*, in *Wikipedia, l'enciclopedia libera*, cit.

([14]) *Internet* ha una struttura a rete basata su una comunicazione di dati mediante la cd. commutazione di pacchetto (*packet switching*), ossia la capacità di frammentare le comunicazioni prodotte da un elaboratore in gruppi di dati («pacchetti»), che vengono inviati in Rete contrassegnati da intestazioni contenenti informazioni sul percorso da effettuare e sull'indirizzo del mittente e del destinatario (indirizzi IP). In Rete vi sono poi degli appositi elaboratori (detti «commutatori di pacchetto») in grado di leggere le suddette intestazioni e di avviare i relativi pacchetti alla destinazione finale. A riguardo cfr. RHEINGOLD, *The Virtual Community*, New York, 1993, p. 74 ss., il quale osserva altresì che è stato creato un sistema a rete «because you don't need a central controller when each racket and the entire network of routers all know how to get information around». La scelta di una struttura a rete, priva di un *computer* centrale di vertice, era stata determinata da ragioni militari, poiché in tal modo un eventuale attacco nemico in grado di distruggere un singolo elaboratore non avrebbe impedito il continuo pieno funzionamento degli altri, cfr. DE LANDA, *War in the age of Intelligent Machines*, New York, 1991, p. 36. In proposito è stato giustamente rilevato da WISE, *Multimedia. A critical introduction*, London-New York, 2000, p. 10, che lo studio scientifico per scopi militari «occupies an important place in western scientific thought and is closely connected with the later development of the *computer*». La diffusissima opinione circa il legame fra l'ideazione di una struttura di comunicazione a rete e le esigenze di difesa militare è stata tuttavia smentita da uno dei padri della rete Arpanet, cfr. VINTON CERF, *La storia di Internet*, 13 settembre 1997, intervista pubblicata su *www.mediamente.rai.it* (visitato il 22 aprile 2005), il quale afferma: «quando fu ideata la prima rete, Arpanet, l'interesse nacque da una necessità di condivisione delle risorse: si volevano collegare i *computer* di circa trenta università in tutto il paese dove si studiava informatica e che ricevevano fondi dall'Arpa. Ciò non aveva niente a che fare con le bombe atomiche, come si suole fantasti-

tarsi dei mezzi necessari per svolgere il proprio ruolo in rete, inserendosi nell'organigramma già esistente mediante accordi contrattuali: l'utente stipula un contratto d'accesso con il *provider* ([15]), il *provider* con i gestori della rete e con i *maintainer* ([16]), i *maintainer* con la *Registration Authority*

---

care... Dopo esserci resi conto che questa tecnologia era molto potente, solo allora cominciammo a porci una serie di domande sul possibile uso della tecnologia di commutazione a pacchetto in ambito militare. Quando, poi, fu ideata *Internet* - il collegamento tra diverse reti - ci ponemmo il problema di renderlo stabile anche in caso di guerra: di far sì, cioè, che se delle bombe avessero distrutto parte della rete, questa si potesse ricollegare da sola automaticamente». Sulle origini di *internet*, fra i tanti, si vedano altresì: NEGROPONTE, *Essere digitali*, Milano, 1997; GATES, *La strada che porta al domani*, Milano, 1996; HAFNER-MARKOFF, *Cyberpunk, Outlaws and Hakers on the Computer Frontier*, New York, 1991.

([15]) L'*access provider* è colui che fornisce agli utenti l'accesso alla rete *internet*; sulla distinzione fra *access provider* e *content provider*, cfr. Articolo 29-Gruppo di lavoro per la tutela dei dati personali dell'Unione europea, *Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-line*, documento adottato il 21 novembre 2000, Bruxelles, p. 11 ss., pubblicato sul sito ufficiale dell'Unione europea *www.europa.eu.int*. Sui contratti di accesso ad *internet* si vedano: BOCCHINI, *Il contratto di accesso ad Internet*, in *Dir. informaz. e informat.*, 2002, p. 471 ss.; ALBERTINI, *I contratti di accesso ad Internet*, in *Giust. civ.*, 1997, II, p. 114 ss.; DE NOVA, *I contratti di accesso ad Internet*, in *Annali it. dir. autore*, 1996, p. 39 ss.

([16]) Per *provider/maintainer*, ai sensi dell'art. 1.1 delle Procedure Tecniche di Registrazione (versione 4.0, attualmente vigente), si intende «colui che ha stipulato un contratto con l'Istituto di Informatica e Telematica del CNR, nelle funzioni di Registro del ccTLD 'it' [vedi nota successiva] per la registrazione per conto proprio o per conto di terzi di nomi a dominio nel ccTLD 'it'». Circa il ruolo della *Registration Authority* si veda la nota successiva, mentre sulla nozione di ccTLD cfr. *infra* nota 27.

([17]) Vengono denominati *Registration Authority* gli organismi, di natura privatistica, competenti per la registrazione e la gestione dei *domain name*. In Italia il ruolo di registrazione dei nomi a dominio «*it*» è stato affidato, nel 1987, dalla IANA (*Internet Assigned Numbers Authority*) all'Istituto CNUCE del CNR, tuttavia, successivamente, si è assistito ad uno sdoppiamento delle strutture di controllo, venendo in essere la *Naming Authority* e la *Registration Authority*, l'una incaricata della formulazione delle regole di assegnazione e gestione dei *domain name*, l'altra delle procedure di registrazione. Nel 2004 tale sistema è stato ricondotto all'unità con l'accentramento di tutte le competenze in capo alla *Registration Authority*, ribattezzata Registro del ccTLD «*it*» e qualificata come «struttura tecnica di servizio» (denominata «Registrazione e gestione nomi a dominio») dell'Istituto di Informatica e Telematica (IIT) del CNR. È stato infatti il Registro a definire il nuovo Regolamento di assegnazione e gestione dei nomi a dominio, in vigore dal 2 agosto 2004, con cui proprio al Registro stesso vengono affidate le competenze inerenti le procedure di riassegnazione dei nomi a dominio, prima in capo alla *Naming Authority*. Su tale recente evoluzione sia concesso rinviare a MANTELERO, *I* domain name *nella giurisprudenza delle corti... fra diritto e tecnologia*, in *Contratto e impresa/Europa*, 2005, n. 1, in corso di pubblicazione.

([17]), la *Registration Authority* con l'ICANN ([18]) o con gli organismi da essa accreditati ([19]). Emerge dunque in maniera evidente l'interoperatività fra le diverse parti di *internet*, non solo sotto il profilo comunicativo, ma anche strutturale, interoperatività manifestata altresì dalla natura contrattuale dei vincoli che legano i diversi soggetti che compongono la rete e dall'ampio ricorso all'autoregolamentazione ([20]).

Da ultimo, conseguenza dei connotati ora descritti, *internet* manifesta un'alta flessibilità, oltre che nel modellarsi, anche nella possibilità di spostare agevolmente i contenuti ivi presenti da un punto all'altro della stessa: trattandosi di *bit*, capaci di essere ugualmente ospitati su qualsiasi *server*, essi possono circolare sull'intera rete senza alcun ostacolo di natura

([18]) L'ICANN (acronimo di *Internet Corporation for Assigned Names and Numbers*) è un ente *no-profit* creato nel 1998 a cui sono state conferite dal Governo statunitense tutte le competenze precedentemente attribuite all'*Internet Assigned Numbers Authority* (IANA), al fine di "privatizzare" la gestione della rete *internet*. Il Dipartimento della Difesa degli Stati Uniti aveva infatti inizialmente affidato alla IANA il compito di gestire gli indirizzi IP, sia sotto il profilo dell'assegnazione degli stessi, sia sotto quello della creazione di nuovi *domain name* di primo livello; la successiva espansione di *internet* negli stati industrializzati diversi dagli USA aveva poi comportato la creazione di tre nuove organizzazioni a cui la IANA aveva delegato la propria competenza in base ad aree geografiche di attribuzione: le *Réseaux IP Européens* (Europa, Medio Oriente ed alcuni stati dell'Africa ed Asia), l'*Asian Pacific Network Information Center* (Estremo Oriente) e l'*American Registry for Internet Numbers* (America settentrionale, centrale e meridionale). In capo alla IANA rimaneva il ruolo di supervisione ed il compito di attribuire agli organismi territoriali i blocchi di indirizzi IP da assegnare. Sulla complessa struttura e sui rapporti esistenti fra i differenti soggetti che concorrono nella gestione e nella regolamentazione della rete *internet*, cfr. PASCUZZI, *Da IANA a ICANN*, in *Foro it.*, 1999, IV, c. 415 ss.; ID., *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, Bologna, 2002, p. 176 ss. e SARTI, *I soggetti di Internet*, in *Annali it. dir. autore*, 1996, p. 5 ss.

([19]) Cfr. sito ufficiale dell'ICANN *www.icann.org*.

([20]) Sulla natura privatistica dei vincoli che legano i diversi soggetti costituenti la rete *internet*, cfr. in dottrina: GALLI, *I domain name nella giurisprudenza*, Milano, 2001, p. 18; SARTI, *Assegnazione dei nomi di dominio e ordinamento statale*, in *Annali it. dir. autore*, 2000, p. 726; ID., *I soggetti di Internet*, cit., p. 17 ss.; FAZZINI, *Il diritto di marchio nell'universo di Internet*, in *Annali it. dir. autore*, 1998, p. 592; MAYR, *I domain names ed i diritti sui segni distintivi: una coesistenza problematica*, in *Annali it. dir. autore*, 1996, p. 233. In giurisprudenza si v. invece: Trib. Bergamo, 6 marzo 2003, in *Dir. informaz. e informat.*, 2003, p. 837 ss.; Trib. Napoli, 26 febbraio 2002, *ivi*, 2002, p. 1005 ss.; Trib. Modena, 27 luglio 2000, in *Giur. merito*, 2001, p. 329 ss.; Trib. Cagliari, 16 aprile 2000, in *Interlex* (*www.interlex.it*, visitato il 10 aprile 2005); Trib. Genova, 17 luglio 1999, in *Dir. informaz. e informat.*, 2000, p. 341 ss. ed in *Dir. e prat. società*, 1999, p. 73 ss.; Trib. Roma, ord., 2 agosto 1997, in *Dir. informaz. e informat.*, 1997, p. 961 ss., in *Dir. ind.*, 1998, p. 138 ss., in *Foro it.*, 1998, I, c. 923 ss. ed in *Arch. civ.*, 1998, p. 952 ss.

tecnica. Diviene così agevole mutare la localizzazione dei materiali *on-line* da un luogo fisico ad un altro, sfruttando la diversa posizione geografica del *server* ospitante.

In sintesi *internet* si presenta come un mezzo di comunicazione accessibile a tutti da ogni luogo (cablato), basato su una struttura non centralmente controllata.

Posto che la regola giuridica è volta a disciplinare quanto accade in una data realtà, occorre interrogarsi se le caratteristiche ora enucleate, oltre ad escludere un controllo proprietario sulla rete, escludano altresì che la stessa sia in qualche maniera controllabile dal legislatore.

È la connotazione strutturale del mezzo di comunicazione che ingenera l'immagine di una *no man land*, è la difficoltà di porre sotto un controllo fisico quanto viene realizzato in *internet* ad indurre la suggestione di un mondo parallelo. Si è infatti in presenza di uno strumento che permette di comunicare senza svelare necessariamente la propria identità, di spostare così velocemente i dati da renderne difficile la localizzazione e la rimozione, e che, da ultimo, opera a livello internazionale in maniera indifferente ai confini geo-politici.

Tutto questo è la rete *internet* ed è proprio da tale natura che derivano i tanti interrogativi posti al giurista e le criticità a cui viene esposto il tradizionale modo di regolare i rapporti intersoggettivi previsto dall'ordinamento.

Sotto il profilo strutturale va poi osservato come gli elementi *software* e *hardware* costitutivi di *internet* (linguaggio html, *router*, indirizzi IP ([21]), *domain name* ([22]), ecc.) non siano neanche essi influenzati da variabili lo-

([21]) L'indirizzo IP è costituito da una serie di numeri, per la precisione si tratta di una sequenza di quattro serie numeriche aventi al massimo tre cifre, ciascuna delle quali è compresa tra 0 e 255; esso serve ad identificare in maniera univoca ogni elaboratore connesso ad *internet*. Tali indirizzi possono avere natura dinamica, variando ad ogni collegamento o durante lo stesso onde favorire l'anonimato dell'utente, oppure statica, identificando in maniera stabile gli *host computer* a cui gli utenti possono accedere per fruire dei servizi o dei contenuti ospitati.

([22]) Il nome a dominio consiste in una sequenza alfanumerica corrispondente in maniera biunivoca all'indirizzo IP (cfr. nota precedente) di un determinato *host computer*, ovvero di un terminale a cui gli utenti possono accedere per fruire di specifici contenuti o servizi sullo stesso ospitati. Sulla corrispondenza biunivoca fra *domain name* ed indirizzo IP dell'*host* cfr. *infra* nota 26. La scelta di dar luogo all'abbinamento fra indirizzo IP e nome a dominio, risalente agli inizi della diffusione della reti informatiche, trova la sua ragione nella difficoltà di ricordare gli indirizzi numerici degli *host*: il ricorso alla denominazione alfanumerica ha infatti notevolmente agevolato gli utenti, favorendo l'impiego di nomi coerenti con il contenuto informativo ed i servizi offerti.

cali, ma diano invece vita ad un tessuto connettivo globale sviluppatosi in maniera autonoma, secondo il solo criterio della funzionalità tecnica. *Internet* ha quindi proprie regole operative, predefinite solamente dai tecnici e, conseguentemente, imposte al legislatore ([23]). Non si tratta tuttavia di semplici *standard* comunicativi, bensì di vincoli strutturali capaci di condizionare in maniera significativa l'agire dei singoli nell'utilizzo del mezzo. Emerge così in maniera evidente il conflitto intrinseco fra norma e struttura, fra ciò che dovrebbe essere e ciò che invece è (o non è) tecnicamente possibile, ove regole pensate per diversi contesti si trovano a coesistere in una nuova realtà tecnologica spesso refrattaria a sottostare ai vincoli di legge.

Un esempio di tale contrasto è rinvenibile nel rapporto fra il sistema di registrazione dei nomi a dominio e la disciplina di protezione dei marchi d'impresa: l'adozione della regola *first come, first served* ([24]) quale criterio fondamentale per l'assegnazione dei nomi a dominio ha infatti messo in crisi i tradizionali principi di specialità e territorialità su cui si fonda la tutela dei segni distintivi ([25]). Tale regola deriva tuttavia da una scelta strutturale posta in essere agli albori delle reti informatiche, quando si decise di catalogare i contenuti accessibili sulla base di un legame biunivoco fra indirizzo IP e nome a dominio ([26]); da tale opzione è necessariamente

([23]) Cfr. REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, in *Texas Law Rev.*, vol. 76, n. 3, February, 1998, p. 553, il quale rileva come nell'era delle reti di telecomunicazioni «for information infrastructure, default round rules are just as essential for participants in the Information Society, as Lex Mercatoria was to merchants hundreds of years ago». In tal senso si v. inoltre REIDENBERG-GAMET-POL, *The Fundamental Role of privacy and Confidence in the Network*, 30 *Wake Forest Law Rev.* 105 (1995) e REIDENBERG, *Governing Networks and Rule-Making in Cyberspace*, 45 *Emory Law J.* 917 (1996).

([24]) Tale regola inibisce l'accoglimento della richiesta di assegnazione di un dato nome a dominio in presenza di una domanda analoga anteriore. Con riguardo alle registrazioni sotto il TLD «*it*», cfr. in tal senso art. 3 del vigente Regolamento di assegnazione dei nomi a dominio (versione 4.0) ed artt. 2.2.1 e 2.4 delle Procedure Tecniche di Registrazione.

([25]) Sul rapporto conflittuale fra l'aterritorialità che caratterizza *internet* e la natura locale dei diritti di privativa si v.: RICOLFI, *I segni distintivi. Diritto interno e comunitario*, Torino, 1999, p. 141; SPADA, Domain names *e dominio dei nomi*, in *Riv. dir. civ.*, 2000, I, pp. 720 e 723 ss.; ID., *La proprietà intellettuale nelle reti telematiche*, *ivi*, 1998, II, p. 640; SENA, *Il nuovo diritto dei marchi*, Milano, 2001, p. 99; ABRIANI, *I segni distintivi*, in ABRIANI-COTTINO-RICOLFI, *Diritto industriale*, in *Tratt. dir. comm.*, diretto da G. Cottino, Padova, 2001, p. 162 ss.; GALLI, *I domain name nella giurisprudenza*, cit., p. 61 ss.

([26]) Fu infatti per iniziativa di Jon Postel, presso l'Università della California di Los Angeles, che venne creata una prima lista degli *host name*, con i relativi indirizzi e l'elenco dei

conseguito uno sviluppo del *Domain Name System* ([27]) che ha reso impossibile la coesistenza di *domain name* identici all'interno del medesimo *Top Level Domain*, cosicché in *internet*, a differenza di quanto accade nella realtà *off-line*, non è dato riscontrare omonimie.

Analogamente, con riferimento al diverso ambito dell'illecito civile, la natura dinamica degli indirizzi IP ([28]) e la possibilità di un accesso in forma anonima alla rete, rafforzate dall'impiego degli *anonimous remailer* ([29]) e dall'impossibilità di conoscere con certezza l'identità di chi si trova al di là del *monitor* ([30]), costituiscono un ostacolo all'applicazione dei criteri di causalità ed imputabilità propri della responsabilità aquiliana.

---

contenuti corrispondenti, al fine di rendere possibile un accesso mirato ai documenti presenti nella rete di ricerca dell'ARPA. In seguito, con l'espandersi della Rete, l'assegnazione e la gestione degli indirizzi IP assunse maggiori proporzioni e venne demandata dal Dipartimento della Difesa degli Stati Uniti prima all'*Internet Assigned Numbers Authority* (IANA) e poi all'*Internet Corporation for Assigned Names and Numbers* (ICANN). Va in proposito però osservato come la IANA consistesse in una funzione (quella di assegnazione dei numeri d'identificazione in *internet*) affidata dal Dipartimento della difesa statunitense (in specie dal DARPA, *Defense Advanced Research Projects Agency*, gestore dell'*Arpanet* di cui *supra* nota 8) all'*Information Sciences Institute della University of Southern California*, sotto la guida di Jon Postel. Prima del passaggio di competenze all'ICANN, nonostante la formale esistenza della IANA, di fatto fu dunque sempre Postel a continuare la propria opera di gestione degli indirizzi IP, in accordo con il governo statunitense. Cfr. altresì *supra* nota 17.

([27]) Onde agevolare le ricerche *on-line*, sin dalla fase iniziale dello sviluppo di *internet* i nomi utilizzati per individuare gli oggetti presenti in Rete sono stati raggruppati facendo uso di specifiche terminazioni (dette *Top Level Domain* o domini di primo livello, il cui acronimo è TLD), differenziate per categorie di contenuti offerti (TLD generici) o per nazionalità della *Registration Authority* (*country code Top Level Domain* o ccTLD). Così i *domain name* registrati presso il Registro del ccTLD italiano avranno tutti come dominio di primo livello «*it*». Sul ruolo del Registro del ccTLD cfr. *supra* nota 17.

([28]) Sulla natura dinamica degli indirizzi IP cfr. *supra* nota 21.

([29]) Si tratta di un servizio offerto in *internet*, mediante il quale i messaggi dei clienti, prima di essere inoltrati ai destinatari, vengono privati dei dati identificativi della provenienza e ritrasmessi, attraverso la sostituzione dell'indirizzo reale di IP con un altro fittizio, diviene così assai difficile poter conoscere la reale provenienza dei dati inviati.

([30]) L'individuazione dell'elaboratore non avviene automaticamente, ma può essere desunta solamente a posteriori. Ravvisato un comportamento illecito realizzato mediante operazioni di *upload* (immissione di contenuti in rete) o di *download* (trasferimento sul proprio *computer* di dati presenti in rete) da un determinato *server*, è possibile, analizzando l'archivio dei *log* dello stesso, conoscere l'indirizzo IP del soggetto connesso e così individuare il *provider* impiegato per l'accesso alla rete. Ogni fornitore d'accesso attribuisce infatti dinamicamente, dunque in modo non permanente, un indirizzo IP all'utente, tuttavia i fornitori attingono tale indirizzo da una serie loro esclusivamente assegnata, è quindi possibile risalire all'*access provider*. Identificato il fornitore d'accesso e l'indirizzo IP, attraverso

La stessa configurazione del *web*, dei *browser* (31) impiegati per l'accesso alla rete e dei motori di ricerca (32), nonché la presenza di specifici elementi *software* – quali, ad esempio, *cookie* (33) e *spyware* (34) –, consentono poi, con particolare riguardo al trattamento dei dati personali, di porre in essere forme di trattamento occulto delle informazioni (35), volte alla defi-

---

il raffronto con i tabulati telefonici indicanti i momenti in cui i diversi utenti si sono collegati al *server*, è poi possibile rintracciare il numero telefonico dell'utente. In tal maniera la cerchia dei possibili responsabili si restringe molto, ma rimane ancor ignota l'identità del soggetto che in concreto ha operato la connessione. Cfr. LESSIG, *Code and other laws of cyberspace*, New York, 1999, p. 32 ss., il quale osserva: «unlike real space, cyberspace reveals no self-authenticating facts about identity. In real space you reveal your sex, your age, how you look, what language you speak, whether you can see, whether you can hear, how intelligent you are. In cyberspace you reveal only an address, and one that has no necessary relationship to anything else about you». La difficoltà di individuare il soggetto responsabile potrebbe indurre a configurare una sorta di responsabilità indiretta in capo al proprietario del *computer*, su cui tuttavia ci si è già interrogati con esito negativo in MANTELERO, *Attività di impresa in Internet e tutela della persona*, cit., p. 43 ss., a cui si permette di rinviare in ragione dell'economia del presente lavoro.

(31) Vengono chiamati *browser* i *software* utilizzati per accedere ad *internet* e per consultare i materiali ivi presenti.

(32) I motori di ricerca sono dei siti *web* che, sulla base degli argomenti indicati dall'utente, sono in grado di selezionare gli indirizzi *web* contenenti le notizie ricercate.

(33) I *cookie* sono dei «marcatori elettronici» consistenti in un insieme di dati inviati dal gestore di un sito *web* al *computer* di chi vi si collega via *internet*. Essi vengono memorizzati sull'*hard disk* dell'utente e raccolgono informazioni personali relative alle connessioni di rete poste in essere da quest'ultimo, le quali sono poi agevolmente «rilette» dal sito *web* che ha inviato il *cookie* o da qualunque suo affiliato. Tali marcatori possono persistere sull'elaboratore a tempo indefinito, oppure avere un termine di scadenza, trascorso il quale divengono inefficaci, o ancora essere dei *cookie* «di sessione», che vengono meno con la cessazione del collegamento alla rete. La funzione originaria dei *cookie* era quella di agevolare l'accesso a siti personalizzati, dove l'utente, identificato per mezzo dei marcatori, non necessitava di registrarsi nuovamente per avere accesso alle notizie di suo interesse, tuttavia è successivamente prevalso un utilizzo distorto di tale tecnologia, volto a conseguire lo scopo, del tutto diverso, di monitorare l'attività di navigazione *on-line* posta in essere da un soggetto. Per una sintetica descrizione sull'impiego dei *cookie* cfr. GAUTHRONET-NATHAN, *On-line services and data protection and the protection of privacy. Study for the Commission of the European Community*, Parigi, 1998, p. 26 ss.

(34) Gli *spyware* sono *software* che consentono l'intrusione in un sistema informatico, permettendo la visualizzazione dei dati ivi presenti, con facoltà di trarne copia, modificarli o distruggerli.

(35) Secondo il Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali, Raccomandazione 1/99 sul trattamento invisibile ed automatico dei dati personali su *Internet* effettuato da *software* e *hardware*, adottato il 23 febbraio 1999, Bruxelles, p. 2, rientrano nell'ambito dei trattamenti occulti «tutti i tipi di operazioni di

nizione di profili individuali funzionali alla commercializzazione di beni e servizi ([36]).

Come emerge da questi sintetici cenni e dalle esemplificazioni riportate, duplice è l'aspetto sotto cui si presenta il problema della regolamentazione di *internet*, coerentemente con i due elementi che caratterizzano ogni mezzo di comunicazione: il mezzo in sé ed il contenuto attraverso lo stesso veicolato.

La struttura tecnico-funzionale di *internet* condiziona infatti *a priori* l'efficacia delle norme la cui applicazione risulti con essa incompatibile, come si è visto in relazione all'impossibilità di trasporre meccanicamente in tale contesto le disposizioni in materia di segni distintivi e come accade con riguardo alla disciplina dei dati personali rispetto alla comunicazione di informazioni posta in essere dai *browser* durante la «navigazione» in rete ([37]).

In linea teorica parrebbe invece più agevole l'attuazione delle norme di legge incidenti sui contenuti diffusi, tuttavia anche in merito a tale aspetto emergono difficoltà non riscontrabili con riguardo ad altri *media*, quali ad esempio la carta stampata. La metodologia con cui i contenuti informativi vengono veicolati *on-line* (frequente è il ricorso all'anonimato), la mobilità delle risorse e l'accessibilità diffusa della rete, costituiscono infatti elementi critici per il ricorso all'apparato normativo esistente, pensato per soggetti quanto meno identificabili, localizzabili ed appartenenti ad un determinato ambito territoriale nazionale ([38]).

---

trattamento attualmente effettuate da *software* ed *hardware* su *Internet* senza che la persona interessata ne sia a conoscenza e che quindi sono per lei 'invisibili'».

([36]) L'attività di «profilazione» consiste nella raccolta del maggior numero di informazioni possibili inerenti i comportamenti, le inclinazioni e le abitudini di un soggetto onde trarne un quadro globale; tale tecnica è attualmente molto utilizzata nell'ambito del *direct marketing* correlato al commercio elettronico. Cfr. Articolo 29-Gruppo di lavoro per la tutela dei dati personali dell'Unione europea, *Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-line*, cit., p. 81 ss., nonché *Federal Trade Commission, Online Profiling: A Report to Congress*, June 2000, rapporto pubblicato sul sito *www.ftc.gov* (visitato il 12 aprile 2005). Si vedano inoltre le osservazioni di RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997, p. 138 ss.

([37]) Cfr. Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali, Raccomandazione 1/99 sul trattamento invisibile ed automatico dei dati personali su *Internet* effettuato da *software* e *hardware*, cit., p. 4.

([38]) Già MAGNI-SPOLIDORO, *La responsabilità degli operatori in Internet: profili interni e internazionali*, in *Dir. informaz. e informat.*, 1997, p. 61, rilevavano che «data la natura 'delocalizzata' ed 'aterritoriale' di *internet*, una prospettiva di diritto interno non è tuttavia esaustiva». A riguardo osserva acutamente PARDOLESI, *La società dei bit*, Roma, 1997, intervista

In tal contesto si può certamente seguitare ad elaborare modelli regolamentari basati sulla fissazione di specifici parametri generali di comportamento, ricorrendo a norme pensate *ad hoc* per *internet* o a quelle vigenti, per poi sanzionare eventuali comportamenti difformi ([39]). Tale soluzione appare tuttavia debole ed incompleta, proprio perché non tiene in adeguata considerazione i limiti posti dal vincolo tecnico-informatico all'efficacia normativa. A mero titolo d'esempio si pensi alla raccolta dei dati personali *on-line* senza il consenso dell'interessato: in questi casi si è sovente in presenza di una vittima dell'illecito assolutamente inconsapevole di quanto accade, ignara della tracciabilità della propria attività in rete o della condivisione da parte di terzi delle informazioni fornite ([40]). Quale incidenza avrà in tal contesto la tutela offerta al singolo dall'ordinamento se questi non è nemmeno in grado di percepire il pregiudizio subito? Analoga considerazione può essere formulata in relazione all'accesso illecito al terminale altrui, reso possibile dalla struttura dei computer e dalla connessione in rete: anche in questo caso la sanzione successiva prevista dall'ordinamento si rivela spesso aleatoria poiché, in assenza di appositi *software* di protezione, il malcapitato rimane completamente all'oscuro dell'accaduto ([41]). D'altra parte può avverarsi anche la situazione opposta, in cui sia del tutto palese la commissione dell'illecito, ma ugualmente inconsistente in termini sostanziali la protezione offerta dal legislatore; così

---

pubblicata su *www.mediamente.rai.it*, come «noi giuristi per primi e forse nella maniera più radicale di altri esperti, verifichiamo la difficoltà di conversione del nostro sapere alla dimensione della digitalizzazione. Il giurista è da sempre stato il giurista municipale ed ha sempre visto con estrema difficoltà il fenomeno del travalicamento delle frontiere, dove il proprio diritto, la propria *expertise* si vanificavano all'improvviso, perché si cambiava diritto al cambiare della carrozza. Insomma, grosso modo oggi la globalizzazione significa evidentemente che il problema diventa un problema giuridico globale. Se noi continuiamo a reclinare su tecniche legate allo specifico, al contesto locale evidentemente non saremo attrezzati neppure per affrontare il problema». Cfr. in tal senso FROSINI, *Il giurista e le tecnologie dell'informazione*, Roma, 1998, p. 110 ss., secondo cui «l'esperienza di *internet* dimostra l'impossibilità di affrontare e risolvere i problemi, che hanno assunto carattere globalizzato,... con le limitate risorse giuridiche di uno Stato o anche di un gruppo di Stati».

([39]) Osserva REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, cit., p. 582: «the reguated-behavior approach provides an indirect but significant stimulus to Lex Informatica norm-construction [...] Behavior regulation leads to a search for the means to assure conforming practices. Technical rules can become a cornerstone of that assurance».

([40]) Cfr. *supra* note 33 e 37.

([41]) Questo è quanto può accadere, ad esempio, in conseguenza dell'impiego di programmi *spyware*, cfr. *supra* nota 34.

nei casi di diffamazione *on-line*, come in quelli di danni da *virus* informatici, spesso le difficoltà tecniche rendono vana o eccessivamente onerosa l'individuazione dei responsabili dell'illecito (42).

Paiono dunque evidenti i limiti di una disciplina che mira unicamente a definire il comportamento vietato, prevedendone la sanzione, incentrata soltanto su un intervento successivo alla commissione dell'illecito, incapace invece di agire preventivamente per impedire il realizzarsi del medesimo (43).

2. - I limiti di quella che potremmo definire regolamentazione «dall'esterno» di *internet* risiedono dunque nella struttura stessa della rete, negli ostacoli frapposti dal dato tecnico all'operatività delle norme; occorre allora chiedersi se a tale approccio non sia possibile affiancare una forma di regolamentazione «dall'interno», incentrata proprio sulla struttura della rete, imponendo un orientamento alla fase progettuale, che comporti uno sviluppo della tecnologia medesima secondo linee evolutive *a priori* compatibili con le regole giuridiche prefissate, tali da impedire *ex ante* i comportamenti vietati (44). Una legislazione tecnica che non sia dunque solamente uno *standard* volto a garantire l'interoperatività dei servizi - come quello che regola il protocollo TCP/IP (45) e le RFC 1591 definite da

(42) Cfr. *supra* nota 30.

(43) Segno delle difficoltà incontrate nella ricerca degli autori delle violazioni dei sistemi informatici è ravvisabile nel crescente ricorso all'adozione di *software* di protezione dei sistemi ed a tecniche di «autodifesa». Tale orientamento è riscontrabile sia tra i proprietari di *home computer*, in genere disposti ad investire scarse risorse nella sicurezza, sia tra le imprese. L'opzione per una tutela preventiva da parte di quest'ultime, dotate di più ampi *budget*, fa riflettere sulla fiducia riposta nell'efficacia delle norme. Teoricamente, anziché pagare uno *staff* di informatici che periodicamente valutino il livello di protezione del sistema attraverso attacchi simulati, le imprese potrebbero infatti impiegare le stesse risorse per intervenire successivamente all'illecito onde rintracciarne i responsabili; la scelta operativa dimostra invece, in maniera implicita, come siano basse le speranze di individuare un soggetto in *internet* e come sia dunque più efficiente cercare di bloccare ogni minima intrusione.

(44) Cfr. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, p. 14: «la tesi della neutralità della tecnologia, sicuramente importante per sottolineare la responsabilità di chi la adopera, trascura il fatto che il concreto ruolo di una tecnologia deriva anzitutto dalla sua forma e dalle sue specifiche modalità d'uso, che contribuiscono a definirne senso e portata sociale. Vi sono effetti che si producono per il solo fatto che si sceglie di ricorrere ad una determinata tecnologia».

(45) Un protocollo informatico di comunicazione consiste in una serie di convenzioni relative alle modalità di scambio delle informazioni ai vari livelli della comunicazione stessa. TCP/IP è l'acronimo di *Transmission Control Protocol/Internet Protocol*, ed è il nome del

Jon Postel per il funzionamento del *Domain Name System* (46) –, ma sia finalizzata a divenire uno strumento per imporre al sistema determinate prassi di comportamento (47), coerenti con il dettato normativo a tutela dei diritti dei singoli.

Va al riguardo precisato che una simile soluzione, in cui la tecnica diviene strumento del diritto per «conformare» la nuova tecnologia a determinati principi, non costituisce un'alternativa netta tendente ad escludere qualsiasi altra modalità di regolamentazione di *internet*, poiché la sinergia fra tecnologia e diritto rappresenta semplicemente un'ulteriore via che merita di essere percorsa accanto alla tradizionale definizione di precisi modelli comportamentali.

Nello specifico paiono poi molteplici i vantaggi correlati all'impiego di tecnologie già «conformate». È infatti indubbio l'innalzamento della soglia di prevenzione che si ottiene inibendo già a livello tecnico la realizzazione dei comportamenti vietati, rendendo così il mezzo stesso inadeguato alla commissione dell'illecito (48); l'efficacia di tale soluzione sarà poi tanto maggiore quanto più risulterà arduo superare la barriera strutturale apposta (49). A ciò si aggiunga, ed è l'aspetto di maggior rilievo, che in questi casi la considerevole riduzione delle violazioni di legge si consegue

---

protocollo affermatosi nel tempo come quello più utilizzato nelle reti informatiche, poiché impiegato dai primigeni nuclei di *internet* (le reti Arpanet e Milnet), a scapito del già vigente *standard* internazionale OSI (*Open System Interconnection*), codificato dal *Consultative Committee for International Telephony and Telegraph* (CCITT), emanazione dell'*International Telecommunications Unions* (ITU), organizzazione affiliata all'ONU.

(46) Cfr. POSTEL, *RFC 1591 - Domain Name System Structure and Delegation*, consultabile al sito *http://faqs.org* (visitato il 25 agosto 2004).

(47) Cfr. REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, cit., p. 555, secondo cui «policymakers can and should look to Lex Informatica as a useful extra-legal instrument that may be used to achieve objectives that otherwise challenge conventional laws and attempts by governments to regulate across jurisdictional lines»; al riguardo l'a. afferma inoltre: «for the development of information policy rules in Lex Informatica, policymakers must use strategies and mechanisms that are different from traditional regulatory approaches».

(48) Cfr. REIDENBERG, *ult. op. cit.*, p. 565: «policy choices are available either through technology itself, through laws that cause technology to exclude possible options, or through laws that cause users to restrict certain actions. Specific information policy technologies that set information flows rules show the significance of Lex Informatica as a parallel rule system».

(49) Così, in ambito privatistico, accade con la tutela del *software*, dove i sistemi di protezione incorporati nel programma rendono impossibile la copiatura o l'illegittimo utilizzo dello stesso, salvo che si riesca a trovare la modalità per rimuovere dette protezioni agendo sul *software* medesimo.

senza far ricorso ad alcuna corte, riducendo in tal modo le controversie in materia di giurisdizione e di diritto applicabile che, a causa della natura sopranazionale di *internet*, spesso affliggono la risoluzione delle liti sorte in rete ([50]).

L'efficienza preventiva delle norme tecniche è d'altra parte già riconosciuta in diversi settori della legislazione statuale - dalla sicurezza dei prodotti alla circolazione stradale - ([51]), nonché nei regolamenti contrattuali di natura privatistica (si pensi ai limitatori di potenza impiegati nella somministrazione energetica od ai dispositivi *software* che impediscono la completa fruibilità di un programma informatico nel caso di licenze a prezzi agevolati, quali ad esempio quelle per studenti).

La possibilità di «conformare» il sostrato tecnologico può inoltre essere sfruttata non solo a fini inibitori, ma anche per rafforzare l'efficacia delle norme comportamentali, specie in relazione ad attività di controllo prodromiche all'intervento sanzionatorio, così l'obbligo di conservazione

([50]) Osserva REIDENBERG, *ult. op. cit.*, p. 572: «the formulation of customized Lex Informatica rules may, to an important degree, avoid many significant difficulties inherent in legal solutions, such as conflict and uncertainty». In merito alle implicazioni connesse alla determinazione della giurisdizione e delle leggi applicabili ai comportamenti posti in essere mediante *internet* cfr. BALLARINO, *Internet nel mondo della legge*, Padova, 1998, *passim* e SICA, *Commercio elettronico e categorie civilistiche*, Milano, 2002, p. 4; con riguardo all'esperienza straniera, in specie statunitense, cfr. invece: ZEKOS, *Internet or electronic Technology: A Threat to State Sovereignty*, 1999 (3) *Journal of Inf. L. Tech.*; BURK, *Jurisdiction in a World Without Borders*, 1 *Va. J.L. & Tech.* 3 (1997); THATCH, *Personal Jurisdiction and the World-Wide Web: Bits (and Bytes) of Minimum Contacts*, 23 *Rutgers Computer & Tech. L.J.* 143 (1997); JOHNSON-POST, *Law and Borders - The Rise of Law in Cyberspace*, 48 *Stan. L. Rev.* 1367 (1996); LESSIG, *The Zones of Cyberspace*, 48 *Stan. L. Rev.* 1403 (1996).

([51]) Un esempio di tale efficienza preventiva si è inoltre riscontrato anche nell'iniziale regolamentazione della registrazione dei nomi a dominio in Italia, ove la regola che limitava la possibilità di registrare «un solo dominio per ciascuna entità» (cfr. versione 2.1 delle Regole di *naming*, par. B.0.7) ha preservato l'ambito del TLD «*it*» dal fenomeno del *cybersquatting* fino al 1999 (per *cybersquatting*, dall'inglese «to squat» ovvero «occupare senza alcuna autorizzazione o permesso», si intende l'attività di chi illegittimamente registra uno o più *domain name* coincidenti con il nome o i segni distintivi altrui). Non è infatti un caso che la scelta di abolire tale limitazione al fine di incrementare le dimensioni del registro italiano dei nomi a dominio (versione 3.1.1 delle Regole di *naming*, in vigore dal 15 dicembre 1999) sia stata accompagnata dal verificarsi di uno dei più massicci fenomeni di *cybersquatting*, posto in essere tra la fine del 1999 e l'inizio dell'anno successivo dall'imprenditore Grauso, su cui si rinvia a MOCCIA, *Grauso e l'incetta di domini: una storia già scritta*, sul sito *www.peacelink.it*, 21 febbraio 2000 (visitato il 16 aprile 2005). In senso conforme alle osservazioni qui espresse cfr. altresì ANTONINI, *La tutela giuridica del nome di dominio*, in *Dir. informaz. e informat.*, 2001, p. 816.

dei *log* (52) da parte dei *provider* può divenire uno strumento utile all'identificazione degli autori degli illeciti commessi *on-line*.

Sotto il profilo operativo, nel definire i parametri tecnici è possibile agire a due diversi livelli, a seconda che si scelga di rendere detti parametri modificabili o meno dall'utente. Qualora infatti si decida di determinare criteri funzionali immodificabili, qualsiasi intento preventivo risulterà rafforzato, tuttavia una simile soluzione comporta precise opzioni di politica legislativa, poiché annulla contestualmente ogni margine di discrezionalità in capo all'individuo, non consentendo uno spostamento né verso l'alto, né verso il basso della soglia di tutela predefinita. Per tale ragione essa si addice maggiormente ai casi in cui si voglia imprimere allo sviluppo tecnologico il rispetto di precise opzioni di fondo, specie quando siano in gioco diritti e libertà fondamentali o norme strutturali del sistema giuridico. Una simile scelta pare dunque consona alla materia dei dati personali, ove infatti, come meglio si vedrà in seguito, la normativa italiana non ha mancato di far ricorso alla definizione di specifici *standard* tecnici (53).

Qualora invece venga riconosciuta all'utente la possibilità di personalizzare l'indice di protezione a cui aspira, verranno valorizzate le eventuali preferenze di quest'ultimo in merito alle scelte dispositive da porre in

(52) I *log* costituiscono la registrazione dei principali dati dei collegamenti di rete effettuati dall'utente, generata automaticamente dal sistema del *server*. I *log* possono essere semplici o molto dettagliati (indicazione del tempo di connessione e dei soggetti con cui ci si è connessi). Funzionalmente l'archivio dei *log* è tenuto per calcolare gli addebiti dei collegamenti, basati su tariffe a tempo, oltre che per individuare i collegamenti sospetti nel caso di tentativi di accesso illecito al sistema o di commissione di altri reati informatici.

(53) Analoghe considerazioni possono essere formulate con riguardo alle modifiche del protocollo di comunicazione impiegato in *internet*: il nuovo protocollo IPv6, sviluppato dall'*Internet Engineering Task Force* (IETF), offre infatti funzioni crittografiche integrate onde assicurare la circolazione dei dati in forma criptata. In questo caso, a differenza di quanto riferito nel testo, l'innalzamento del livello di tutela è imposto a tutti gli utenti non in virtù dell'intervento normativo, a seguito di accordi internazionali, bensì in conseguenza di una scelta operata dagli informatici che si occupano di sviluppare l'architettura della rete *internet*. In tal senso emerge un dato comune all'evoluzione delle reti informatiche, per cui molteplici aspetti nevralgici della gestione e dello sviluppo delle stesse, sebbene rilevanti per milioni di persone, vengono decisi da una *elite* « illuminata », la cui legittimazione è tale solo in quanto costituiscano davvero la rappresentazione ai massimi livelli della collettività di soggetti interessati alla funzionalità della rete. Un così vasto potere di influire con soluzioni tecniche sui criteri di comunicazione lasciato in mano a pochi, sebbene di eccezionale competenza, appare tuttavia un rischio in ragione delle dimensioni assai notevoli degli interessi economici e politici che imprese e singoli governi hanno nel controllo della rete *internet*.

essere. A tal proposito si possono richiamare le funzioni già previste nei comuni *browser* di navigazione in *internet*, che consentono di fissare il grado di condivisione di determinati dati, nonché di manifestare eventuali restrizioni alla ricezione di *cookie*.

Rispetto ai due livelli di tutela così delineati pare rinvenibile anche nella regolamentazione tecnica la distinzione fra norme (tecniche) imperative e dispositive, in ragione delle possibili opzioni date all'utente (54). Ne consegue dunque un differente ruolo dei soggetti chiamati a definire gli *standard* in esame, a seconda che rilevi il profilo della determinazione degli stessi o quello delle scelte applicative: mentre parrebbe opportuno che la codificazione della moderna *lex informatica* avvenisse secondo indicazioni provenienti da fonti legislative, al fine di conformare il profilo tecnologico a quello normativo, diversamente le scelte eventuali circa le regole tecniche «dispositive» potrebbero essere espressione della negoziazione fra i soggetti differentemente coinvolti nel dar vita ad *internet* (*software house*, *provider*, società di telecomunicazione, utenti, ecc.), con conseguente maggior rilievo delle dinamiche di mercato (55).

3. - Un interessante «laboratorio d'analisi» di quanto sin qui esposto è costituito dalle soluzioni tecniche approntate per garantire la tutela dei dati personali, onde far fronte al sempre più rilevante fenomeno della profilazione degli utenti di *internet* (56).

In tale settore si sono infatti sviluppate le cd. PET (acronimo di *privacy enhancing technologies*), ovvero applicazioni *software* o *hardware* vol-

(54) A tal riguardo occorre altresì distinguere a seconda che i dispositivi tecnici siano posti a monte o a valle della struttura informatica: mentre nel primo caso essi incideranno direttamente sulla configurazione della rete ed in quanto tali non potranno essere facilmente aggirati dai singoli utenti, nel secondo caso interesseranno le funzionalità dei terminali dell'utente (es. *software* capaci di assicurare un determinato livello di tutela dei dati personali), risultando così più agevolmente manipolabili da quest'ultimo. Specularmente la prima soluzione preclude la personalizzazione degli *standard* di tutela, mentre la seconda permette rilevanti margini di discrezionalità nella scelta del livello di protezione preferibile.

(55) In merito cfr. anche REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, cit., p. 573. Sul ruolo del legislatore non mancano tuttavia osservazioni critiche in dottrina, oggetto di più ampia disamina nella parte conclusiva del presente lavoro.

(56) Sul concetto di profilazione e sulle diverse tecniche con cui tale obiettivo si realizza in *internet*, nonché sulle implicazioni giuridiche in tema di protezione dei dati personali, sia consentito rinviare, in ragione dell'economia del presente lavoro, a quanto espresso in MANTELERO, *Attività di impresa in Internet e tutela della persona*, cit., p. 146 ss. ed ai riferimenti ivi citati.

te ad impedire o limitare l'accesso alle informazioni inerenti l'utente ([57]). L'interazione fra tali tecniche e la normativa in materia di dati personali risulta positiva in quanto le stesse consentono all'interessato di disporre dei propri dati in maniera discrezionale, dando luogo ad una gradazione nell'accesso e non comportando necessariamente l'unica soluzione dell'anonimato, che potrebbe non rivelarsi funzionale alle esigenze del singolo ([58]). Dal punto di vista pratico tale risultato si ottiene inserendo un intermediario fra il soggetto interessato ed i terzi richiedenti le informazioni, detto intermediario disporrà del profilo dell'utente ed avrà il compito di filtrare le domande ([59]) in base alla conformità del potenziale richiedente ad un profilo predeterminato o interpellando volta per volta l'utente, anche in presenza di trattamenti occulti. Il potenziamento di tali sistemi di «negoziazione» del consenso verso forme di automatismo, onde ridurre il ruolo dell'utente alla sola definizione dei criteri di massima, potrebbe poi essere raggiunto ove trovassero applicazione specifici *standard* di certificazione dei siti *web*, capaci di classificare la natura, le finalità, le modalità e le tipologie dei trattamenti posti in essere.

Con riguardo alle applicazioni volte a consentire un accesso differenziato ai dati personali, così come per quanto concerne il ricorso ad eventuali strumenti crittografici, l'adozione delle tecniche di tutela può conse-

---

([57]) Diverse soluzioni applicative vengono descritte già nel primo documento di lavoro in materia elaborato dall'Articolo 29-Gruppo di lavoro per la tutela dei dati personali dell'Unione europea, intitolato *Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-line*, cit., p. 87 ss. Con riguardo all'impiego delle PET cfr. altresì RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, cit., p. 147.

([58]) Va al riguardo riconosciuto come la definizione dei profili possa infatti rivelarsi utile in termini di pre-selezione delle offerte commerciali.

([59]) La natura dell'intermediario può variare, essendo possibile ricorrere ai *proxy-server* o agli agenti *software*. Nel primo caso si ha un sito sul quale risiede in forma criptata il profilo dell'utente: sarà il *proxy-server* a selezionare i siti *web* che collimano con il profilo definito, eventualmente tenendo conto di precise indicazioni ricevute dall'utente in materia di accesso e divulgazione dei dati. Cfr. inoltre *Working Group* on «Data Protection in Telecommunications» *of the Committee on* «Technical and organisational aspects of data protection» *of the German Federal and State Data Protection Commissioners*, *Privacy Enhancing Technologies in Telecommunications*, approvato nell'ottobre del 1997, p. 5 ss. Sui *proxy-server* in generale si v. Articolo 29-Gruppo di lavoro per la tutela dei dati personali dell'Unione europea, *Documento di lavoro relativo ai servizi di autenticazione on-line*, adottato il 29 gennaio 2003, Bruxelles, p. 3 ss. Diversa è invece l'operatività degli agenti *software*: si tratta di programmi «intelligenti» in grado di decidere autonomamente rispetto agli ordini ricevuti dall'utente. Mediante tali agenti, ricorrendo allo sfruttamento delle PET, l'utente di *internet* può delegare agli stessi il compimento di attività complesse *on-line* limitando l'accesso ai propri dati personali.

guire sia da un'opzione in tal senso del legislatore, sia da una volontà spontanea dei privati: si ripropone anche in questo contesto l'interrogativo sulla scelta del soggetto chiamato a definire gli *standard* tecnici (60).

Nello specifico il d. lgs. n. 196 del 2003 risolve il dilemma in favore del legislatore, fissando i principi generali secondo cui il dato tecnico andrà «conformato» al fine di renderlo compatibile con il livello (minimo) di tutela ivi richiesto. Tale soluzione pare coerente con la natura stessa della materia disciplinata, attinente agli aspetti di maggior rilievo della persona e per questo non suscettibile di essere apprezzata secondo una mera dinamica di mercato (61). Neanche l'affermarsi delle connotazioni più marcatamente patrimoniali e negoziali del diritto sui dati (62) può infatti indurre lo

(60) Sullo sviluppo da parte dei privati di tecniche volte alla tutela dei dati personali, il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali della Commissione europea, nel parere n. 1/98 del 16 giugno 1998, dal titolo *Piattaforma per le preferenze in materia di protezione della vita privata (P3P - Platform for Privacy Preferences) e la norma aperta per i profili (OPS - Open Profiling Standard)*, p. 2, ha osservato: «una piattaforma tecnica per la protezione della vita privata non sarà di per sé sufficiente a garantire tale protezione sul *Web*. Occorre che una piattaforma del genere sia applicata in un quadro di regole esecutive sulla tutela dei dati, in grado di fornire a tutti un livello minimo e non negoziabile di protezione della vita privata». Cfr. altresì Articolo 29-Gruppo di lavoro per la tutela dei dati personali, *Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-line*, cit., p. 93 ss. Nella specie la piattaforma per le preferenze in materia di protezione della vita privata (*P3P - Platform for Privacy Preferences*) rimetteva la determinazione del livello di tutela dei dati personali al comune accordo fra l'utente di *internet* ed il sito *web* interessato al trattamento. Nel parere n. 1/98 del Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali della Commissione europea, cit., p. 2, si legge in proposito: «il principio di base [del funzionamento della P3P] prevede che l'utente acconsenta alla raccolta dei suoi dati personali da parte di un sito (l'*Open Profiling Standard* è volto a fornire la trasmissione sicura di un profilo standard di dati personali), solo se le pratiche dichiarate del sito in termini di protezione della vita privata (per esempio le finalità della raccolta dei dati, l'eventuale uso a fini secondari o la cessione a terzi) soddisfano le esigenze dell'utente».

(61) In proposito osserva Rodotà, *Tecnologie e diritti*, cit., p. 55: «dovendosi ormai considerare il tema della *privacy* come parte integrante della più generale dimensione della garanzia dei diritti civili e dell'organizzazione della democrazia, gli interessi in questione non sono riducibili alla sfera individuale e, comunque, esprimono valori irriducibili alla pura logica proprietaria»; nello stesso senso cfr. anche Rodotà, *L'insidia contro la privacy è una sfida per tutti, planetaria*, in *Telèma*, 2001. Si veda inoltre Alpa, *Il "diritto dei computers"*, in Aa.Vv., *Le banche dati in Italia. Realtà normativa e progetti di regolamentazione*, Napoli, 1985, p. 7, per il quale «non è possibile rassegnarsi all'idea che il mercato possa 'fare da sé', in una sorta di *bricolage* normativo, quasi che solo i portatori d'interesse possono sapere quali sono le regole con cui disciplinare quegli stessi interessi».

(62) Cfr. Alpa, *La disciplina dei dati personali. Note esegetiche sulla legge 31 dicembre 1996*

Stato ad abdicare al suo fondamentale ruolo di tutela dei cittadini, specie con riferimento ad un settore così sensibile, anche in relazione all'esercizio dei diritti politici (63). A ciò si aggiunga che nella comunicazione *on-line* i processi di raccolta e di elaborazione dei dati si fanno più subdoli e nascosti, consentendo altresì di ignorare qualsiasi legge di mercato in favore di una logica di rapina (64); proprio in tale contesto l'individuo non può dunque essere lasciato solo senza che gli venga assicurato un livello minimo di protezione mediante la previsione di specifiche limitazioni legali all'impiego dei dati personali.

In tal senso il d. lgs. n. 196 del 2003, imponendo l'adozione di adeguate misure strutturali volte ad agevolare l'esercizio del diritto di accesso (65), optando per la preferenza per forme di trattamento che garantiscano l'anonimato (66), nonché formulando apposite indicazioni in materia di obblighi informativi (67), implica necessariamente l'adozione di determinati *standard* operativi che incidono direttamente anche sui mezzi tecnici utilizzati (68). È poi innegabile che la stessa suddivisione delle competenze

---

n. 675 e successive modifiche, Roma, 1998, p. 10, il quale constata come, nell'attuale contesto socio-economico, «l'informazione, in quanto tale, è divenuto strumento di profitto». Sulla *commodification* dei dati personali cfr. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, cit., pp. 151 e 155, nonché SIMITIS, *Il contesto giuridico e politico della tutela della privacy*, in *Riv. crit. dir. priv.*, 1997, p. 573 e ZENO-ZENCOVICH, *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium Juris*, 1997, p. 469.

(63) Con espresso riferimento alle implicazioni inerenti la tutela dei diritti politici dei cittadini cfr. RODOTÀ, *ult. op. cit.*, p. 152 ss., il quale osserva come «[la *privacy*] si presenta, infine, come precondizione della cittadinanza dell'età elettronica e, in quanto tale, non può essere affidata unicamente alla logica dell'autoregolamentazione o ai rapporti contrattuali».

(64) Cfr. CARIDI, *La tutela dei dati personali in Internet: la questione dei logs e dei cookies alla luce delle dinamiche economiche dei dati personali*, in *Dir. informaz. e informat.*, 2001, p. 769, il quale con riguardo al «mercato dei dati» che si realizza *on-line* osserva: «si tratta però di un mercato singolare, in cui ad una 'domanda' consapevole e mirata si contrappone una 'offerta' nella migliore delle ipotesi caratterizzata dall'inconsapevolezza di cedere un prodotto avente un valore economico [...] ovvero, nelle ipotesi più gravi ed ancora purtroppo frequenti, caratterizzata dalla totale inconsapevolezza di cedere dei dati personali».

(65) Cfr. art. 10, commi 1°, 2° e 6°, d. lgs. n. 196 del 2003.

(66) Cfr. artt. 3 e 11, comma 1°, lett. *e*), d. lgs. n. 196 del 2003.

(67) Cfr. art. 13, d. lgs. n. 196 del 2003.

(68) Così ad esempio la necessità di poter raccogliere il consenso dell'interessato solamente dopo che lo stesso sia stato adeguatamente informato ai sensi dell'art. 13, d. lgs. n. 196 del 2003, comporta il ricorso a specifiche tecniche di realizzazione della pagina *web* attraverso l'impiego di appositi *link* o di *frame* la cui mancata consultazione inibisca la possibilità di manifestare il consenso al trattamento dei dati personali. Nel linguaggio informatico il *link* consiste nel collegamento ipertestuale che consente il passaggio da una pagina *web*

fra i soggetti autori del trattamento, sia verticale ([69]) che orizzontale ([70]), comporti implicitamente il ricorso a dispositivi di autenticazione volti ad impedire attività di gestione che esulano da ciascun ambito funzionale.

Il ricorso ad una forma di regolamentazione che faccia un uso più marcato del potere di «conformare» il sostrato informatico emerge poi in maniera più netta nelle norme concernenti le misure minime di sicurezza di cui all'art. 33, d. lgs. n. 196 del 2003 ([71]), come manifestato dalla stessa scel-

---

ad un'altra, mentre il *frame* costituisce una delle sezioni in cui può essere divisa una pagina *web*, in maniera tale da poter scorrere separatamente l'una dall'altra mostrando contenuti differenti.

([69]) Cfr. artt. 28, 29 e 30, d. lgs. n. 196 del 2003, ove si stabiliscono diversi livelli operativi per titolare, responsabili ed incaricati del trattamento, precisando altresì la necessità per i responsabili e gli incaricati di agire secondo le istruzioni loro impartite.

([70]) Si avrà una suddivisione delle competenze in senso orizzontale nelle ipotesi in cui siano nominati più responsabili del trattamento o più incaricati.

([71]) Con riguardo alla sicurezza dei dati già l'art. 31, d. lgs. n. 196 del 2003 impone un obbligo generale di adottare le misure di sicurezza che si rendano necessarie onde prevenire ed evitare «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». La mancata ottemperanza a tale indicazione legislativa rileva sotto il profilo civilistico in virtù del disposto dell'art. 15 T.U., che configura un'ipotesi di responsabilità fondata sull'art. 2050 c.c. per i danni cagionati per effetto del trattamento dei dati, essendo le misure di sicurezza indubbiamente una, se non la principale, delle «misure idonee a evitare il danno». Va in proposito rilevato come parte della dottrina, con riguardo all'analogo richiamo dell'art. 2050 c.c. già contenuto nell'art. 18, l. n. 675 del 1996, abbia osservato che la finalità principale di tale rinvio non fosse tanto quella di qualificare come «pericolosa» l'attività di trattamento dei dati personali, quanto quella di offrire una migliore tutela giudiziaria al soggetto leso, grazie all'inversione dell'onere probatorio ed alle limitazioni di prova derivanti dall'applicazione dell'art. 2050 c.c. Cfr. in tal senso: ALPA, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in *Dir. informaz. e informat.*, 1997, p. 722; GRANIERI, *Una proposta di lettura sulla tutela risarcitoria nella vicenda del trattamento dei dati personali*, in *Danno e resp.*, 1998, p. 222; CARUSI, *La responsabilità*, in *La disciplina del trattamento dei dati personali*, a cura di V. Cuffaro e V. Ricciuto, Torino, 1997, p. 361. In senso difforme si v.: ZENO-ZENCOVICH, *I diritti della personalità dopo la legge sulla tutela dei dati personali*, cit., p. 468; SICA, *Art. 18*, in GIANNANTONIO-LOSANO-ZENO-ZENCOVICH, *La tutela dei dati personali. Commentario alla legge 675/1996*, Padova, 1997, p. 183 e, con specifico riferimento alla normativa vigente, BRAVO, *Le condizioni di liceità del trattamento*, in *Il codice in materia di protezione dei dati personali*, a cura di J. Monducci e G. Sartor, Padova, 2004, p. 65. Va inoltre aggiunto che, come sottolineato dal Garante per la protezione dei dati personali, parere 22 marzo 2004, in *www.garanteprivacy.it*, l'inosservanza dell'obbligo posto dall'art. 31, d. lgs. n. 196 del 2003 rende di per sé illecito il trattamento, anche in assenza di un danno per gli interessati, ed inoltre viola il diritto fondamentale alla protezione dei dati personali riconosciuto ad ognuno. Il richiamo dell'art. 2050 c.c., unito all'esplicito riferimento alle «conoscenze acquisite in base al progresso tecnico» di cui all'art. 31, d. lgs. n. 196 del

ta di ricorrere alla predisposizione di un apposito disciplinare tecnico ([72]). Al riguardo già l'art. 34 prevede in via generale cinque diverse tipologie di interventi tecnici volti ad assicurare un corretto trattamento dei dati sotto diversi profili: la verifica sulla legittimità dell'accesso da parte dei soggetti incaricati del trattamento ([73]), la protezione fisica degli archivi e del loro contenuto da accessi illegittimi ([74]), la prevenzione rispetto alle ipotesi di perdita dei dati ([75]), la prevenzione generale dei rischi ([76]), l'adozione di tecniche crittografiche per le informazioni maggiormente sensibili, inerenti la salute e la sessualità ([77]). Il solo esame di queste indicazioni generali contenute nella norma mostra chiaramente come i principi di liceità e correttezza del trattamento ed i limiti soggettivi correlati al consenso manifestato trovino attuazione mediante la realizzazione di un contesto materiale caratterizzato dall'adozione di misure tecniche ed informatiche volte a renderne impossibile, o quanto meno difficile, la violazione.

Nel dettaglio, l'allegato *B* prevede poi esplicitamente il ricorso a tecniche informatiche quali le credenziali di autenticazione ([78]), precisandone inoltre la natura - *password*, dispositivi *ad hoc* o dati biometrici ([79]) - ed indicando i criteri da seguire nella formulazione delle parole chiave ([80]). Analogo ricorso ad una regolamentazione «dall'interno» si ha al fine di

---

2003, costituiscono poi ulteriori elementi indicativi della propensione ad avvalersi della tecnologia al fine di conseguire effettivamente il livello di tutela offerto dalle disposizioni normative. Con riguardo al rilievo dello stato della tecnica nella valutazione della responsabilità *ex* art. 2050 c.c., si v.: TRIMARCHI, *Rischio e responsabilità oggettiva*, Milano, 1961, p. 277; MONATERI, *Le fonti delle obbligazioni, 3. La responsabilità civile*, in *Tratt. dir. civ.*, diretto da R. Sacco, Torino, 1998, p. 1035; FRANZONI, *La responsabilità del "provider"*, in *Resp. comunicazione impresa*, 1997, p. 767 ss. e ID., *Il danno da attività pericolose nella giurisprudenza*, in *questa rivista*, 1985, p. 155 ss.

([72]) Cfr. all. *B* al d. lgs. n. 196 del 2003.

([73]) Cfr. art. 34, lett. *a*), *b*), *c*) e *d*), d. lgs. n. 196 del 2003.

([74]) Cfr. art. 34, lett. *e*), d. lgs. n. 196 del 2003.

([75]) Cfr. art. 34, lett. *f*), d. lgs. n. 196 del 2003.

([76]) Cfr. art. 34, lett. *g*), d. lgs. n. 196 del 2003.

([77]) Cfr. art. 34, lett. *h*), d. lgs. n. 196 del 2003. Si v. inoltre le specifiche indicazioni tecniche contenute nelle regole da 20 a 24 dell'all. *B* al d. lgs. n. 196 del 2003, riguardanti sia i dati sensibili che quelli giudiziari.

([78]) Cfr. regola 1 e seguenti dell'all. *B* al d. lgs. n. 196 del 2003.

([79]) Cfr. regola 2 dell'all. *B* al d. lgs. n. 196 del 2003.

([80]) La regola 5 dell'all. *B* al d. lgs. 196 del 2003, detta indicazioni analitiche in proposito, fissando in otto caratteri la lunghezza della parola chiave, salvo i limiti tecnici dello strumento elettronico impiegato, ed imponendo che si tratti di parola priva di «riferimenti agevolmente riconducibili all'incaricato».

prevenire comportamenti intrusivi ai danni di banche dati informatizzate, imponendo l'adozione obbligatoria di *software* di protezione (sia rispetto agli accessi illegittimi che agli attacchi di virus informatici) e di programmi atti a correggere gli eventuali difetti del sistema ed a prevenirne la vulnerabilità, con periodico aggiornamento degli stessi ([81]).

Maggiori specificazioni riguardano poi la sicurezza in senso proprio dei dati, poiché, oltre al salvataggio delle informazioni con frequenza almeno settimanale ([82]), viene altresì richiesta dalla legge la predisposizione di un apposito documento programmatico sulla sicurezza contenente l'indicazione delle misure approntate al fine di garantire un livello globale di sicurezza del trattamento ([83]). Tale ultima misura, che riguarda solo i trattamenti di dati sensibili o giudiziari effettuati con l'ausilio di strumenti elettronici ([84]), è chiaramente incentrata sull'analisi tecnica dei rischi di danneggiamento, alterazione o distruzione delle informazioni e sull'adozione di apposite modalità di gestione in grado di scongiurare tali eventi. Il testo normativo impone dunque la conformità della strumentazione utilizzata per l'elaborazione dei dati a specifiche indicazioni di massima (dalla protezione dei locali ([85]) ai programmi di ripristino ([86]), ai sistemi di cifratura ([87]) dei dati).

La funzione svolta da tali disposizioni tecniche ([88]) assume un ruolo

---

([81]) Cfr. regole 16 e 17 dell'all. *B* d. lgs. n. 196 del 2003.

([82]) Cfr. regola 18 dell'all. *B* d. lgs. n. 196 del 2003.

([83]) L'obbligo di redigere e di tenere aggiornato tale documento deriva dal disposto dell'art. 34, lett. *g*), d. lgs. n. 196 del 2003. Cfr. altresì la regola 26 dell'all. *B* al d. lgs. n. 196 del 2003 ove si prevede che dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza venga dato conto nella relazione d'accompagnamento del bilancio d'esercizio, ove prevista.

([84]) Cfr. regola 19 dell'all. *B* al d. lgs. n. 196 del 2003. Già la previgente disciplina prevedeva il documento programmatico sulla sicurezza, ma solamente in relazione al trattamento di dati sensibili o relativi a determinati provvedimenti giudiziari effettuato mediante elaboratori accessibili tramite una rete di telecomunicazioni disponibile al pubblico, cfr. art. 6, d.p.r. n. 318 del 1999 ed artt. 22 e 24, l. n. 675 del 1996. L'attuale struttura del documento programmatico sulla sicurezza risulta inoltre ampliata rispetto a quella definita sotto la vigenza della l. n. 675 del 1996, specie con riguardo ai criteri ed alle modalità di ripristino dei dati e di cifratura degli stessi di cui alle regole 19.5 e 19.8 dell'all. *B*.

([85]) Cfr. regola 19.4 dell'all. *B* al d. lgs. n. 196 del 2003.

([86]) Cfr. regola 19.5 dell'all. *B* al d. lgs. n. 196 del 2003.

([87]) Cfr. regola 19.8 dell'all. *B* al d. lgs. n. 196 del 2003.

([88]) Alle disposizioni richiamate nel testo, valide in generale per i trattamenti posti in essere avvalendosi di strumenti elettronici, vanno aggiunte le specifiche previsioni di cui all'art. 32, d. lgs. n. 196 del 2003, relative ai soli fornitori di un servizio di comunicazione elettronica accessibile al pubblico, dunque ai *provider*. In tali casi la sicurezza dei dati non riguarda infatti solamente i contenuti informativi ospitati sulle pagine *web*, ma altresì i dati

cardine nell'attuazione della disciplina concernente la tutela dei dati personali, così mostrando l'opportunità di avvalersi della stessa tecnologia per creare contesti operativi conformi al dettato normativo. Quanto previsto nel d. lgs. n. 196 del 2003, dall'obbligo dell'informativa al requisito del consenso dell'interessato, alla suddivisione dei ruoli fra i diversi autori del trattamento, verrebbe infatti ad essere vanificato in assenza di un'adeguata considerazione dei profili attinenti la sicurezza. Elevare il livello di tutela nelle fasi di raccolta ed elaborazione dei dati risulterebbe inutile se poi le medesime informazioni fossero custodite in maniera negligente, esposte al rischio di essere conosciute da soggetti non legittimati, fatte possibile oggetto di alterazione o distruzione. Proprio tale funzione centrale, la messa in sicurezza dei dati ed in generale delle operazioni di trattamento, non viene realizzata dal legislatore mediante semplici enunciazioni di norme di diligenza, ma passa attraverso la regolamentazione tecnica degli aspetti di maggiore criticità, ricorrendo alla predisposizione di applicazioni idonee ad evitare il danno o a ridurne gli effetti. È in tal contesto che appaiono poco propizi i continui rinvii a cui sono state sottoposte le disposizioni riguardanti la completa attuazione dell'obbligo di adozione del documento programmatico sulla sicurezza, per altro ricorrendo sistematicamente alla decretazione d'urgenza ([89]).

---

relativi al traffico ed all'ubicazione (definiti dall'art. 4, comma 2°, lett. *h* ed *i*), nonché più in generale la sicurezza dei servizi e delle comunicazioni elettroniche. Emerge così chiaramente la componente dinamica correlata alla fornitura di servizi attraverso la rete, non a caso le misure di sicurezza dovranno riguardare non solo le strutture del fornitore del servizio ma anche le strutture della rete pubblica di comunicazioni (cfr. art. 32, comma 2°). Anche con riguardo ai *provider* rileva dunque in maniera significativa il ricorso alla regolamentazione tecnica, sia come attuazione dei suddetti obblighi di sicurezza, sia sotto il profilo del monitoraggio dei rischi e della predisposizione delle misure strumentali atte a prevenirli, come dimostrato dall'ultimo comma dell'art. 32.

([89]) Cfr. Garante per la protezione dei dati personali, *Relazione 2004. L'attuazione del Codice nel quadro della Costituzione Europea*, p. 3 ss., ove il ricorso alle continue proroghe dei termini per adottare le misure minime di sicurezza è stimmatizzato come un segnale «in controtendenza rispetto al progetto di 'stabilizzare' le regole di protezione dei dati personali», sottolineando come «nel pur breve lasso di tempo dall'entrata in vigore del Codice, ricorrendo alla decretazione d'urgenza, si sono differiti i termini per l'adempimento di taluni obblighi posti a garanzia dell'interessato, relativamente all'applicazione delle 'nuove' misure minime di sicurezza». Al riguardo va ricordato come il previgente d.p.r. n. 318 del 1999 prevedesse già l'adozione di misure minime di sicurezza ed in specie l'art. 6 di detto decreto stabilisse l'obbligo di redigere il documento programmatico sulla sicurezza per tutti coloro che effettuassero trattamenti di dati sensibili o giudiziari servendosi di elaboratori accessibili mediante una rete di telecomunicazioni disponibile al pubblico, obbligo che og-

4. - L'esempio dell'interazione fra norme giuridiche e tecnologia offerto dalla disciplina in materia di dati personali mostra come la sinergia fra diritto e tecnica consenta altresì al legislatore, come al giurista, di abbandonare la condizione di muto spettatore del progresso, costretto ad una continua «rincorsa» (spesso vana) di tale evoluzione, svolgendo più un ruolo di censore rispetto a quanto già in essere che una funzione propositiva e di guida rispetto a quanto in fase di progettazione o di realizzazione.

Se dunque dal servirsi della tecnica quale strumento per una regolamentazione preventiva e maggiormente vincolante dei fenomeni più strettamente connessi allo sviluppo dell'ingegno umano si possono trarre dei giudizi positivi, occorre altresì indagare i limiti di tale *modus operandi*, per poi affrontare da ultimo il più complesso interrogativo circa i soggetti legittimati a porre dette regole tecniche.

Con riguardo al primo profilo va osservato che alcuni caratteri di *internet* si impongono come predefiniti rispetto a qualsiasi intervento regolamentare. In questo contesto, come in altri, si è dunque in presenza di regole tecniche aventi natura strutturale ed in quanto tali non suscettibili di essere «conformate» senza mettere in discussione la stessa realtà che si vuole disciplinare. Così, riprendendo l'esempio del *Domain Name System*, appare insuperabile il limite della corrispondenza biunivoca fra indirizzo IP e nome a dominio, fonte di significative restrizioni all'utilizzo di segni distintivi identici (90). Analogamente è implicita nella stessa struttura a rete l'impossibilità, o quanto meno l'estrema difficoltà, di limitare la diffu-

---

gi è invece esteso anche a chi si avvalga di elaboratori non connessi alla rete pubblica, cfr. *supra* nota 84. In tal senso l'art. 180, comma 1°, d. lgs. n. 196 del 2003 fissava al 30 giugno 2004 il termine per l'adozione delle misure minime indicate nel testo unico che non si fosse già tenuti ad adottare in virtù del d.p.r. n. 318 del 1999, dunque anche per il documento programmatico per la sicurezza nel caso dei soggetti tenuti a redigerlo per la prima volta, a cui il Garante aveva equiparato in via interpretativa anche «chi, già dotato di un DPS redatto o aggiornato nel 2003, ritenga necessario utilizzare un trimestre in più, rispetto al prossimo 31 marzo, per curare la stesura di un testo significativo e più impegnativo nella ricognizione dei rischi e degli interventi previsti», cfr. Garante per la protezione dei dati personali, parere, 22 marzo 2004, pubblicato sul sito ufficiale dell'Autorità garante *www.garanteprivacy.it*. Detto termine, ad oggi, è stato fatto oggetto di un triplice rinvio, attuato dapprima dall'art. 3, d.l. 24 giugno 2004, n. 158 (convertito con l. 27 luglio 2004, n. 188), quindi dall'art. 6, d.l. 9 novembre 2004, n. 266 (convertito con l. 27 dicembre 2004, n. 306) e da ultimo dall'art. 6 *bis*, d.l. 30 dicembre 2004, n. 314 (convertito con l. 1° marzo 2005, n. 26), con conseguente slittamento dall'iniziale 30 giugno 2004 al 31 dicembre 2005.

(90) Si rinvia in proposito ai richiami di dottrina e giurisprudenza indicati in MANTELERO, *I* domain name *nella giurisprudenza delle corti... fra diritto e tecnologia*, cit.

sione di contenuti illeciti, potendo gli stessi essere spostati con estrema facilità da un punto all'altro di internet pur rimanendo sempre accessibili a ciascun utente.

Rispetto a queste ipotesi ed in generale a tutte quelle in cui non pare possibile «conformare» l'elemento tecnico, non resta che l'unica via della regolamentazione «dall'esterno», attraverso la tradizionale apposizione di obblighi e divieti di comportamento secondo uno schema precettivo-sanzionatorio.

A tali considerazioni va poi aggiunto che in diversi casi lo sviluppo di tecnologie capaci di facilitare l'attuazione del dettato normativo si scontra con le logiche del sistema produttivo, poiché richiede l'assunzione di costi non compatibili con la commercializzazione dei prodotti, tali da spingere piuttosto le imprese a rinunciare all'applicazione stessa della tecnologia che si vuole «conformare». Così è stato ad esempio per i dispositivi di identificazione a radiofrequenza (91) rispetto allo sviluppo di nuovi modelli in grado di fornire un elevato livello di protezione dei dati personali (92): il ricorso ad efficienti sistemi crittografici è al momento escluso poiché eleverebbe a tal punto i costi di produzione di detti dispositivi da renderli insuscettibili di collocazione sul mercato (93).

---

(91) Gli identificatori a radio frequenza o RFID (secondo l'acronimo della dizione in lingua inglese), comunemente detti anche *e-tag* (*electronic-tag*) o *smart-tag*, consistono in minuscole etichette elettroniche (le più piccole raggiungono dimensioni dell'ordine di un terzo di millimetro) capaci di memorizzare e trasmettere dati ad appositi lettori mediante l'impiego di onde radio. Tali dispositivi RFID possono essere «passivi», in grado di inviare dati solo se appositamente sollecitati dal lettore e dotati di un ridotto raggio d'azione, oppure «attivi», capaci di operare autonomamente, inviando informazioni e creando reti comunicative con altri dispositivi.

(92) In proposito si rinvia a quanto più diffusamente osservato in MANTELERO, *Identificatori a radiofrequenza (RFID) e controllo capillare dei dati personali: il rischio di un "mondo nuovo" per il consumatore?*, in *Contratto e impresa/Europa*, 2004, p. 15.

(93) Cfr. in tal senso JUELS-RIVERST-SZYDLO, *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*, 2003, p. 5, in *http://theory.lcs.mit.edu* (visitato il 15 marzo 2004) e JULES-PAPPU, *Squealing Euros: Privacy protection in RFID-enabled banknotes*, 2003, p. 3, in *www.rsasecurity.com* (visitato il 15 marzo 2004). Solo recentemente sono apparsi studi più possibilisti sull'adozione di sistemi crittografici, sebbene risultino opinioni ancora isolate; cfr. a riguardo *Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology*, 19 gennaio 2005, Bruxelles, p. 17, ove viene richiamato lo studio di FELDHOFER-DOMINIKUS-WOLKERSTORFER, *Strong Authentication for RFID Systems using the AES Algorithm*, in *Lecture Notes in Computer Science (LNCS)*, vol. 3156, Springer Verlag, 2004, p. 357 ss. Cfr. altresì AIGNER-FELDHOFER, *Secure Symmetric Authentication for RFID Tags*, 2005, pubblicato sul sito *http://tcmc.tugraz.at* (visitato il 28 marzo 2005) e BONO-GREEN-STUBBLEFIELD-JUELS-RUBIN-SZYDLO, *Security Analysis of a Cryptographically-Ena-*

Proprio quest'ultima riflessione induce ad esaminare il punto più controverso della regolamentazione mediante il ricorso a regole tecniche, ovvero la determinazione dei soggetti legittimati a fissare tali *standard*. Secondo un primo orientamento, emerso ad esempio in merito alla diffusione delle PET, sarebbe il mercato a condizionare ed a determinare l'adozione di specifiche regole tecniche corrispondenti agli interessi dei singoli, dovendosi negare un analogo ruolo al legislatore (94). Seguendo invece una diversa linea interpretativa si potrebbe ritenere che spetti al legislatore fissare il quadro normativo di base all'interno del quale le disposizioni tecniche si giustappongono, come è avvenuto con riguardo al d. lgs. n. 196 del 2003 in materia di dati personali.

Rispetto a queste alternative la soluzione può forse trovarsi in una via intermedia, che tenga conto della particolarità di *internet* e degli interessi tutelati. Come già si è osservato in maniera incidentale, ove questi ultimi attengano agli aspetti di maggior rilievo, quali la persona umana, le libertà fondamentali, la repressione di comportamenti illeciti, l'ordine pubblico economico, è difficile escludere la necessità e l'opportunità di un intervento da parte del legislatore e non pare preferibile rimettere ogni decisione alle regole del mercato, la cui efficienza non è per altro insuscettibile di dubbi. Diversamente in contesti marcatamente caratterizzati da dinamiche commerciali e dall'autonomia dei contraenti, sembra condivisibile come anche la codificazione di *standard* tecnici possa considerarsi coerente con le scelte di mercato (95). D'altra parte le due soluzioni non paiono doversi considerare necessariamente in maniera alternativa, essendo immaginabile anche un'integrazione fra le stesse, in conformità alla tendenza verso una regolamentazione di *internet* che unisca ad alcuni elementi normativi di fonte statuale altri di fonte autoregolamentare (96).

---

bled RFID Device e JUELS, *Minimalist Cryptography for Low-Cost RFID Tags*, entrambi pubblicati sul sito *www. rsasecurity.com* (visitato il 28 marzo 2005).

(94) Cfr. LESSIG, *Code and other laws of cyberspace*, cit., p. 160 ss. e, *contra*, ROTENBERG, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, in 2001 *Stan. Tech. L. Rev.* 1, si veda in specie § 90 ss.

(95) Si pensi in proposito alle forme di certificazione dei siti *web* secondo parametri prescelti dai diversi enti certificatori, in rapporto ai potenziali interessi delle diverse categorie di utenti, su cui cfr. Articolo 29 - Gruppo di lavoro per la tutela dei dati personali dell'Unione europea, *Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-lin*e, cit., p. 94.

(96) Sul ruolo dell'autoregolamentazione cfr. GIORDANO, *Invoking Law as a Basis for Identity in Cyberspace*, 1998 *Stan. Tech. L. Rew.* 1; GIBBONS, *No Regulation, Government Regulation, or Self-regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 *Cornell J.L. & Pub. Pol'y* 457 (1997).

La stessa natura sovranazionale della rete *internet*, con la conseguente difficoltà di assicurare con certezza l'attuazione pratica del dettato legislativo anche ove esso si concretizzi in applicazioni tecniche, comporta infatti la necessità di un coinvolgimento diretto dei soggetti che agiscono in rete e che sono artefici della struttura della stessa. Occorre dunque valorizzare le dinamiche volte alla condivisione di comuni scelte operative, collocandole però all'interno di un più ampio quadro normativo nazionale e, auspicabilmente, internazionale ([97]), specie ove vengano in gioco interessi non suscettibili di essere ridotti ad una mera logica di scambio.

In tale quadro il valore aggiunto del ricorso alla regolamentazione attraverso la tecnologia rivela un ulteriore elemento di forza, consistente nella maggior facilità di rendere comuni e condivise analoghe strutture tecniche, rispetto alla più difficile integrazione e circolazione dei modelli giuridici.

La vastità di diffusione della rete *internet* e la diversità degli ordinamenti degli stati interessati, unite alla pluralità degli operatori coinvolti ed alla mancanza di una struttura verticistica, pongono infatti innegabili resistenze all'individuazione di norme per tutti identiche, mentre proprio l'uniformità strutturale di *internet* può rivelarsi un elemento connettivo su cui operare in maniera concertata per la fissazione di alcuni *standard* generali volti a facilitare o ad ostacolare specifici comportamenti di fatto. In tal contesto il ricorso alla «conformazione» della tecnologia potrebbe dunque rivelarsi non un'alternativa, ma certamente un efficace ausilio rispetto alla consueta regolamentazione «dall'esterno» delle nuove realtà derivanti dal progresso della scienza applicata.

([97]) Osservava in proposito SANTANIELLO, *I fattori evolutivi della privacy*, relazione tenuta al «Forum P.A. 2001», Roma, 7-11 maggio: «l'evoluzione normativa dell'intera materia non può affidarsi più a una fonte legislativa monocentrica, bensì a un policentrismo di fonti, collocate in una coordinata sequenza a vari livelli (una cornice legislativa concertata fra tutti gli Stati interessati alla soluzione del problema e, in aderenza ad essa, la specificazione di regole mediante le leggi nazionali, a seconda delle varie aree geografiche, e inoltre l'adozione di codici-modello, di formazione auto-disciplinare). Si realizza in tal modo quel moderno processo regolatore, frutto della convergenza di molteplici fonti normative, che si definisce come *coregulation*». Si v. inoltre: SICA, *Commercio elettronico e categorie civilistiche*, cit., p. 4; COSTANZO, *La magistratura sfida Internet. A margine di un caso francese, ma non solo...*, in *Dir. informaz. e informat.*, 2001, p. 227; FROSINI, *Il giurista e le tecnologie dell'informazione*, cit., p. 111 ss.; MAGNI-SPOLIDORO, *La responsabilità degli operatori in Internet: profili interni e internazionali*, cit., p. 61. In argomento cfr. altresì la relazione della commissione d'inchiesta governativa francese, operante fra il novembre del 1999 ed il maggio del 2000 su incarico del Primo Ministro Jospin, *Du droit et des libertés sur l'internet. La corégulation, contribution française pour une régulation mondiale*, p. 15.