Informatica e diritto, XXXV annata, Vol. XVIII, 2009, n. 1, 301 p.

Diritti di libertà nel mondo virtuale della rete

a cura di

Marina Pietrangelo

Informatica e diritto
Rivista internazionale

XXXV annata - Seconda serie - vol. XVIII (2009) - n. 1
Periodicità semestrale (max 500 pagine annuali)

Direzione e redazione
ITTIG / CNR
Via dei Barucci, 20 - 50127 Firenze
tel.: 055 43995 - fax: 055 4399605
rivista@ittig.cnr.it - www.ittig.cnr.it/

Amministrazione
Edizioni Scientifiche Italiane s.p.a.
via Chiatamone - 780121 Napoli
tel.: 081 7645443 - fax: 081 7646477
info@edizioniesi.it - www.edizioniesi.it

La rivista è organo dell'Istituto di Teoria e Tecniche dell'Informazione Giuridica del Consiglio Nazionale delle Ricerche (già Istituto per la documentazione giuridica)
Direttore: C. Ciampi; *Comitato d'Istituto:* F. Bargellini, A. Cammelli, P. Catalano, C. Ciampi, R.M. Di Giorgi, E. Fameli, S. Faro, R. Nannucci, M. Ragona, P. Spinosa, D. Tiscornia

Dattiloscritti, libri da recensire – possibilmente in duplice esemplare – pubblicazioni periodiche in cambio vanno spediti esclusivamente all'indirizzo della Casa editrice. Estratti in prosieguo di stampa o anticipati, eventualmente richiesti all'atto della consegna dei dattiloscritti, saranno forniti a prezzo di costo. La maggior spesa per le correzioni straordinarie è a carico dell'autore.

Registrazione presso il Tribunale di Napoli al n. 4379 del 22/3/93. Responsabile: Costantino Ciampi. Iscritta a Registro Nazionale della Stampa in data 29/7/85 al n. 1635. Spedizione in abbonamento postale art. 2 comma 20/b legge 662/96 filiale di Napoli.
Periodico esonerato da B.A.M. art. 4, 1° comma, n. 6, d.P.R. 627 del 6-10-78.

DIRITTI DI LIBERTÀ NEL MONDO VIRTUALE DELLA RETE

Prefazione

Desidero anzitutto ringraziare il Direttore ed il Comitato scientifico della Rivista "Informatica e diritto" per avermi sostenuta nel lavoro di curatela di questo numero speciale, dedicato ad un tema assai complesso, oltre che particolarmente ampio e sfaccettato, che abbiamo voluto riassumere nell'espressione "diritti di libertà nel mondo virtuale della Rete".

Forti della "complicità" dell'evento mediatico, vista cioè la risonanza avuta dalla pronuncia del Tribunale di Milano relativa al caso Google, e visto anche l'accesso dibattito che tale pronuncia ha occasionato sulla Rete, abbiamo ritenuto utile aprire un ulteriore spazio di riflessione, in cui i tanti spunti emersi di recente potessero approdare a nuovi e più maturi approfondimenti. L'attenzione è diretta evidentemente alle molteplici questioni di natura giuridica che la Rete genera, coinvolge, se non travolge.

Con nostro grande piacere, l'invito a sottomettere contributi proposto nei mesi scorsi ha suscitato vivo interesse sia in Italia che all'estero, a nostro avviso evidenziando ancora una volta, se necessario, l'immutata ansia esplorativa dello studioso di diritto per il tema sensibile dei diritti, anche e ancor più in questa nostra età della Rete.

Con questa nuova modalità di acquisizione dei contributi da pubblicare, più di trent'anni dopo l'uscita del suo primo numero, la Rivista ha così voluto rinnovarsi, oltre che mediante la ridetta modalità della *call for paper*, anche e specialmente nell'articolazione delle sue rubriche e nelle tematiche da privilegiare. Com'è noto ai suoi lettori, infatti, la Rivista ha da sempre prestato grande attenzione alla speciale natura del rapporto tra tecnica e diritto, costituendo tale rapporto la sede naturale delle discipline cui la Rivista stessa è dedicata, cioè il "diritto dell'informatica" e "l'informatica giuridica". E in questo numero speciale è proprio all'origine di tale rapporto che essa torna a dedicarsi, trattandosi di un rapporto articolato ed affascinante al contempo, che l'avvento di Internet ha reso negli anni ulteriormente complesso, ponendolo sovente all'attenzione dei giuristi per la mole di questioni nuove che esso ha saputo sollevare.

Ci piace qui ricordare gli interrogativi suggeriti nell'invito, perché in fondo essi tracciano già, pur se in forma interrogativa, la linea degli argomenti approfonditi nei saggi raccolti in questo numero.

Qual è il ruolo odierno delle norme in relazione allo sviluppo tecnologico? Quanto ancora i nostri legislatori s'illudono di poter regolare la tecnica? La nuova tecnologia è forse assurta da materia regolata a principio regolatore? I vecchi istituti giuridici hanno retto all'avvento di Internet? Come sono cambiati i diritti della persona? Quali nuove realtà hanno richiesto di essere giuridicamente regolate? Quanto ha contribuito Internet alla diffusione dei saperi e delle conoscenze?

Nella cornice offerta dai quesiti richiamati, la *call* proponeva tracce puntuali, per un verso, plasmate sui vecchi istituti degli ordinamenti contemporanei, che hanno tentato di adeguarsi alla nuova realtà tecnologica; per altro, orientate a sollecitare riflessioni sui nuovi scenari generati da Internet che, pur non richiedendo di essere giuridicamente regolati, presentano comunque non pochi risvolti di natura squisitamente giuridica. Le ricordiamo a futura memoria, anche e soprattutto perché vedremo che ad alcune di tali tracce, più che ad altre, è andata la maggiore attenzione dei nostri autori: la tutela della persona; il diritto alla riservatezza dei dati personali; il diritto d'autore; la tutela del consumatore; la disciplina giuridica dei *domain names;* la regolazione giuridica dei siti Web; i profili giuridici dei s*ocial network;* la tutela dei contenuti; la responsabilità degli Internet *providers*; la sicurezza in Internet; il rapporto tra la *governance* della Rete e la sua regolazione giuridica.

Come anticipato, molti sono stati i contributi pervenuti in risposta all'invito, e voglio qui ringraziare particolarmente tutti gli autori, sia coloro i cui lavori sono stati ammessi alla pubblicazione, sia anche coloro che in questa occasione non hanno trovato spazio, con l'auspicio di future collaborazioni.

Senza pretesa di valutazioni statistiche, si può affermare che gli argomenti che hanno riscosso maggiore "successo" sono stati due: la *Internet governance* (Abba e Trumpy, De Grazia, Martino, Nicotra e Rossi) e la *privacy (*Messina, Mifsud-Bonnici, Pagallo e Vaciago). Non pochi sono stati anche i lavori dedicati ai profili dell'Internet di seconda generazione, con spunti di carattere più generale (Badocco, Di Donato e Pellerino) o più puntuali (Bassoli e De Vivo).

In molti casi la medesima questione è affrontata da due o più autori, nel rispetto dello spirito della *call*, finalizzato all'acquisizione dei migliori contributi, anche se vertenti sullo stesso tema d'indagine. Il nostro obiettivo, infatti, non è stato quello di trattare *tutte* le tracce proposte, ma piuttosto quello di proporre riflessioni originali, anche tra loro divergenti, esplorando semmai solo alcuni dei temi suggeriti.

Così, sul tema della *Internet Governance* le considerazioni proposte sono ricche e poliedriche: esse affrontano, in taluni casi, aspetti più squisitamente giuridici; in altri, questioni più propriamente di natura tecnica. Non mancano poi considerazioni di carattere storiografico o approfondimenti mirati su specifici istituti, quale quello della disciplina giuridica dei nomi a dominio.

Come ci ricordano, tra gli altri, Abba e Trumpy, la *Internet governance* è "lo sviluppo e l'applicazione da parte dei governi, del settore privato e della società civile, nei loro rispettivi ruoli, di principi, norme, regole, procedure decisionali e programmi condivisi che determinano l'evoluzione e l'uso di Internet"[1].

Si tratta di questioni di tale rilevanza da non poter essere più ignorate dal giurista, che – interessato al fenomeno globale della Rete e a tutti i risvolti che l'esigenza di un nuovo "diritto globale" impone - comincia ad occuparsene, affiancando l'operato e le riflessioni dei tecnici che per primi hanno colto l'entità di tale questione. È dunque un piacere ospitare in questo numero più d'un contributo sul tema, anche alla luce dell'attuale dibattito sulla proposta di un nuovo "Codice Azuni" per Internet[2] e in vista del prossimo *Internet Global Forum*, che si terrà nel mese di settembre 2010 a Vilnius in Lituania[3].

[1] V. la nota 1 del par. 1 del contributo richiamato.

[2] Si tratta di una iniziativa avviata in Italia nel mese di agosto 2010 dal Ministro per la pubblica amministrazione e l'innovazione, Renato Brunetta. Citando testualmente il documento denominato per l'appunto "Codice Azuni versione beta. Per una governance di Internet", il fine ambizioso dell'iniziativa è quello di mettere insieme tutti gli *stakeholders* per favorire un processo di regolamentazione concertato e condiviso 'dal basso'" così da approdare alla "elaborazione, in modo collaborativo, di un contributo condiviso, che definisca principî e strumenti atti a gestire in modo armonioso lo sviluppo della Rete e la nascita di una 'tangibile' cittadinanza digitale globale, entrambe comunque saldamente fondate sulla tutela dei diritti della persona". Tutte le informazioni sono reperibili sul sito http://www.azunicode.it/.

[3] Cfr. http://www.intgovforum.org/

Molto articolata anche la sezione sulla tutela della riservatezza dei dati personali, in cui sono presenti approfondimenti su profili specifici, quali il diritto all'oblio o la relazione tra la *privacy* ed il *design,* ma anche analisi più generali in cui sono comparati gli istituti di tutela presenti in diversi ordinamenti. Si tratta di riflessioni nuove, in taluni casi davvero intriganti, che prospettano soluzioni originali nell'approccio a questioni apparentemente note e sedimentate.

D'altro canto, quello della *privacy* è un tema tanto sviscerato quanto da sviscerare, vista la sua natura di corollario essenziale di tutti i discorsi su una sempre più mutante società dell'informazione. Ben vengano, dunque, nuove e più attente riflessioni in materia, considerati i repentini mutamenti della tecnica ed il loro impatto con gli istituti giuridici posti a presidio della sfera dei diritti della persona. In tal senso, ad esempio, è sufficiente pensare alla difficile tenuta della nostra legislazione sulla *privacy* dinnanzi alle odierne più avanzate tecniche di incrocio dei dati personali, tecniche che le vigenti norme sull'anonimizzazione faticosamente riescono a fronteggiare[4].

Alle prime due sezioni se ne affianca poi una terza, che raccoglie analisi originate dalle caratteristiche del cosiddetto Web 2.0, dedicate in parte a questioni di rilevanza generale, e in parte a temi più specifici, quale quello dei *social network*, "luogo" su cui gli utenti di Internet trascorrono sempre più tempo.

Si tratta, a nostro avviso, di saggi accomunati dal medesimo approccio alle questioni trattate: in essi cioè si ragiona dei profili giuridici dei più vari fenomeni tecnici con grande perizia, districandosi all'interno del quadro normativo vigente, ma senza mai indulgere in rivendicazioni legislative di sorta. In tali contributi è, infatti, ravvisabile un'idea comune, che - per citare Lessig – consiste nell'approcciare i profili tecnici sempre e comunque con un atteggiamento di umiltà normativa (*regulatory humility*)[5].

[4] V. già P. OHM, *Broken promises of privacy. Responding to the surprising failure of anonymization,* 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

[5] Cfr. il discorso di Lawrence Lessig, tenuto alla Camera dei deputati l'11 marzo 2010 su http://webtv.camera.it/portal/portal/default/Archivio?IdEvento=387&IdIntervento=814.

Ma non voglio trattenere ulteriormente il lettore con queste note introduttive, certa dell'interesse che i lavori di seguito proposti susciteranno in esso.

Con l'augurio di una felice lettura.

Marina Pietrangelo
Ricercatrice Ittig-Cnr

L'Internet *Governance*

La *enhanced cooperation* per le politiche pubbliche di gestione delle risorse critiche di Internet

ABBA LAURA, STEFANO TRUMPY*

1. PREMESSA

Scopo di questo articolo è fornire un quadro di riferimento che possa contribuire a comprendere le questioni che muovono intorno al processo della *enhanced cooperation* sulla gestione delle risorse critiche di Internet e ai ruoli e alle responsabilità dei Governi del mondo nella definizione, coordinamento e implementazione di politiche pubbliche per la Rete.

La *enhanced cooperation*, concepita come un processo che riguarda il potenziamento delle sinergie fra le istituzioni globali che si occupano di Internet *governance* in senso stretto[1], prefigura azioni e impegno di tutti gli *stakeholders*[2] della Rete verso una maggiore collaborazione all'interno del sistema, sia per

* Gli Autori sono esperti di *governance* di Internet; Laura Abba è dirigente tecnologo presso l'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche (IIT-CNR); Stefano Trumpy è rappresentante del Governo italiano nelle organizzazioni internazionali che si occupano di Internet *governance*.

[1] La Internet *governance* è lo sviluppo e l'applicazione da parte dei governi, del settore privato e della società civile, nei loro rispettivi ruoli, di principi, norme, regole, procedure decisionali e programmi condivisi che determinano l'evoluzione e l'uso di Internet (Art. 34 *Tunis Agenda for the Information Society*; 18-11-2005 WSIS-05/TUNIS/DOC/6 http://www.itu.int/wsis/docs2/tunis/off/6rev1.html). In senso stretto di *governance*, l'evoluzione e l'uso di Internet dipende dai protocolli TCP/IP e dalla gestione del sistema di indirizzamento. Gli attori principali sono la *Internet Corporation for Assigned Names and Numbers* (ICANN), la *Internet Society* (ISOC), l'*Internet Engineering Task Force* (IETF) e l'*International Telecommunication Union* (ITU). Vedi L. ABBA, C. COSMATOS, *Global Internet Governance: un nuovo campo di ricerca interdisciplinare riguardo all'Internet del futuro*, in "Informatica e diritto", n. 1-2, 2008, pp. 497-506.

[2] Gli *stakeholder* della Rete – in italiano si traduce "portatori di interesse della Rete" – possono essere suddivisi in tre categorie: società civile globale – che include utenti e il mondo tecnico-scientifico degli sviluppatori della rete –, settore privato e governi.

lo studio di politiche pubbliche sia per il consolidamento dei principî, che stanno alla base del funzionamento della Rete.

Negli anni recenti i capi di Governo hanno riconosciuto che Internet è un elemento centrale dell'emergente società dell'informazione, essenziale per il mantenimento delle funzioni vitali della società come la salute, la sicurezza e il benessere economico e sociale dei cittadini. Tuttavia, pur essendo universalmente riconosciuto che stiamo trattando un sistema globale – dove le questioni di politica pubblica richiedono accordi internazionali e non a caso sono argomento nell'agenda dell'ONU – esistono punti di vista diversi sull'adeguatezza dei meccanismi e delle attuali istituzioni globali che gestiscono i processi e sviluppano le politiche per Internet[3].

Sulla costruzione della società dell'informazione, l'ONU organizzò il vertice mondiale WSIS 2003-2005. Dal vertice sono risultati quattro documenti finali[4]:

- Geneva Declaration of Principles;
- Geneva Plan of Action;
- Tunis Commitment;
- Tunis Agenda for the Information Society.

Da questi documenti emerge con chiarezza il fatto che le politiche pubbliche per Internet sono una questione di ordine internazionale: a partire dalle svariate faccende legate allo sviluppo della società dell'Informazione sino al riconoscimento che tutti i governi devono partecipare alla Internet *governance* su base paritetica per garantire la stabilità e la sicurezza del sistema e la continuità dei servizi.

[3] Al centro delle discussioni c'è l'attività che ruota intorno a ICANN, ISOC, IETF e ITU. Su questi attori e sui rappresentanti dei governi nazionali ruota la possibilità di intervenire per fissare i criteri che consentano alla Rete di funzionare, attraverso la migliore collaborazione degli enti citati.

[4] Il vertice mondiale sulla Società dell'Informazione si è svolto in due fasi. La prima fase è stata ospitata a Ginevra nel dicembre 2003, la seconda a Tunisi nel novembre 2005. I documenti finali sono disponibili sul sito dell'ITU alla sessione www.itu.int/wsis/documents/. Significativo è stato in particolare il secondo Vertice di Tunisi. È stata definita la così detta *enhanced cooperation* per le risorse critiche di Internet ed è stato avviato il processo dell'*Internet Governance Forum*, un Forum che discute annualmente i temi della Internet *governance* intesi in senso allargato e quindi che comprendono anche l'aspetto dei contenuti e quelli legati alla infrastruttura di rete. Vedi www.itu.int/wsis/index.html.

In particolare, dal vertice WSIS del 2005 esce la raccomandazione rivolta al Segretario generale dell'ONU di coinvolgere i Governi e le organizzazioni internazionali che partecipano alla gestione di Internet in un processo di *enhanced cooperation* che miri a garantire che i governi stessi possano, su base paritetica, espletare il loro ruolo e le loro responsabilità nelle questioni di politica pubblica di gestione delle risorse critiche di Internet. Il documento di riferimento è la *Tunis Agenda for the Information Society*. Come è stato dimostrato dal tempo occorso al Segretario generale dell'ONU per adempiere a questo suo mandato, la definizione di tale processo di cooperazione, è uno dei temi attuali più critici e delicati della Internet *governance*. Nella comunità internazionale esiste infatti una grande varietà di pareri difficilmente armonizzabili: alcuni sono a favore di una partecipazione più diretta dei governi nella gestione dell'Internet, per altri – come il governo italiano – basterebbe invece accrescere la presenza dei governi all'interno delle esistenti organizzazioni internazionali che gestiscono la Rete.

2. Le quattro aree fondamentali di politica pubblica correlate alla Internet *governance*

Per la complessità degli aspetti connessi all'evoluzione della Internet *governance*, al termine delle negoziazioni del primo vertice WSIS del 2003, fu attivato un gruppo di esperti per lavorare ad un Rapporto[5] che presentasse le diverse opzioni e catalogasse i diversi problemi. Nel Rapporto si è inteso il problema della *governance* della Rete in senso largo, non limitandosi all'identificazione delle sole questioni di politica pubblica collegate alle risorse critiche di Internet, ma esteso a problemi fondamentali per il futuro di Internet come la sicurezza, la proprietà intellettuale, l'estensione dell'accesso alla rete, il multilinguismo, solo per nominarne alcuni. Basandosi su un lavoro di accertamento dei fatti, il rapporto ha definito quattro aree fondamentali di politica pubblica della Internet *governance*:

[5] Ci si riferisce al WGIG - *Working Group on Internet Governance* (www.wgig.org), al quale presero parte rappresentanti dei governi, del settore privato e della società civile. Per informazioni sui lavori del gruppo e sul testo in italiano del Rapporto si vedano le pubblicazioni di V. Bertola, *Futuro della gestione internazionale di Internet*, Quaderno edito da ISOC Italia, agosto 2005 (www.quadernionline.it).

1. questioni legate all'infrastruttura e alla gestione di risorse critiche di Internet, incluse l'amministrazione del sistema dei nomi a dominio e degli indirizzi dell'Internet Protocol (indirizzi IP), l'amministrazione del sistema dei *root server*, gli standard tecnici, l'interconnessione e lo scambio di traffico alla pari (*peering*), le infrastrutture di telecomunicazione tra cui le tecnologie innovative e convergenti, ed anche l'introduzione del multilinguismo. Queste sono questioni di rilevanza diretta per la Internet *governance* che ricadono nell'ambito di organizzazioni esistenti che ne sono responsabili;

2. questioni legate all'uso di Internet, inclusi lo *spam*, la sicurezza della rete e il crimine *on-line*. Per quanto queste questioni siano direttamente correlate alla *governance* di Internet, la natura della cooperazione globale da esse richiesta non è ben definita;

3. questioni che sono legate a Internet, ma con un impatto molto più ampio di Internet, dove si hanno organizzazioni esistenti responsabili per tali questioni, come i diritti di proprietà intellettuale (IPRs) o il commercio internazionale;

4. questioni legate agli aspetti della Internet *governance* correlati allo sviluppo, ed in particolare la costruzione di capacità nei Paesi in via di sviluppo.

Il processo di *enhanced cooperation* è stato attivato per risolvere una buona parte delle questioni del primo gruppo. Alle altre questioni non corrisponde al momento un'istituzione o un processo *ad hoc* per la loro risoluzione, tuttavia sono argomenti che tutti gli *stakeholders* della Rete hanno bene in evidenza e sui quali ci si confronta da tempo all'interno dell'Internet Governance Forum (IGF)[6].

3. La *enhanced cooperation* per le risorse critiche

Il termine *enhanced cooperation*, apparso per la prima volta nelle discussioni sulle politiche pubbliche di Internet al vertice WSIS di Tunisi del 2005, ad oggi non ha ancora trovato una chiara definizione e applicazione come processo all'interno del sistema di *governance* di Internet.

[6] Vedi par. 6.

In altri contesti, come quello dell'Unione europea, con *enhanced cooperation* ci si riferisce ad una specifica procedura[7], introdotta dal Trattato di Amsterdam nel 1999, che consiste in un accordo fra almeno un terzo dei Paesi UE (oggi, almeno nove) per cooperare su un tema di loro interesse nel quadro giuridico comunitario, approvando una legge europea che si applica esclusivamente nei Paesi in questione, senza però discriminare gli altri e lasciandoli liberi di aggregarsi all'iniziativa in un momento successivo. Una procedura inventata dieci anni fa, solo oggi ha trovato un'applicazione concreta. Scavalcando un blocco ormai insormontabile al Consiglio, quattordici Stati membri, fra cui l'Italia, si sono messi d'accordo in questi giorni per cooperare fra loro al fine di facilitare i divorzi "transfrontalieri"[8].

Tornando al sistema Internet, quando nel 2005 si definì, il processo della *enhanced cooperation* si riconobbe il bisogno di una cooperazione sul tema del coordinamento e gestione delle risorse critiche di Internet, senza però che fosse chiaro come e quali accordi di cooperazione dovessero essere messi in atto per armonizzare le specifiche azioni intraprese dai governi per affrontare i problemi sorti[9].

[7] Nell'Unione europea la *enhanced cooperation* è un processo ufficiale che permette una cooperazione più stretta tra un numero di Paesi su un determinato tema di politica pubblica. Si tratta di una misura eccezionale, valida come "ultima spiaggia" quando è impossibile trovare un accordo per o contro una certa proposta in sede di Consiglio (fra i 27 governi). Per entrare in vigore, ci deve essere comunque l'approvazione della maggioranza del Consiglio e della Commissione, e il via libera del Parlamento. Uno Stato membro non può opporsi alla creazione di una *enhanced cooperation*. In linea di principio un numero minimo di nove Stati membri deve partecipare ad un processo di *enhanced cooperation*, che rimane però aperto a qualunque altro Stato membro desideri parteciparvi. Il processo non deve costituire una discriminazione tra gli Stati che partecipano e gli altri (http://europa.eu/scadplus/glossary/enhanced_cooperation_it.htm).

[8] UE Brussels, 24.3.2010 *Implementing Enhanced Cooperation in the Area of the Law Applicable to Divorce and Legal Separation.* Il documento è consultabile all'indirizzo http://ec.europa.eu/justice_home/news/intro/doc/com_2010_105_en.pdf.

[9] WSIS di Tunisi 2005 - Tunis Agenda Par. 69: "We further recognize the need for enhanced cooperation in the future, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters, that do not impact on international public policy issues".

Appaiono lecite le domande che la comunità della rete si pone. Seguiremo l'approccio che vuole raggruppare i governi che credono nello sviluppo *multi-stakeholder* delle politiche per la Rete? Creeremo un accordo che all'inizio non sarà universalmente condiviso ma aperto a chi lo vorrà condividere in futuro? La stessa procedura sarà seguita da quei governi che vedono un rafforzamento del loro ruolo all'interno di ICANN? Un accordo iniziale sarà trovato fra quei governi che sono convinti che l'autoregolamentazione sia l'unica soluzione da seguire? Ovvero una cooperazione sarà stabilita fra quei numerosi Paesi in via di sviluppo, secondo cui Internet dovrebbe introdurre politiche pubbliche d'impostazione dirigistica, come quelle attuate nella tradizionale regolamentazione internazionale delle telecomunicazioni, con processi decisionali puramente governativi?

Fin dalla chiusura dei lavori di Tunisi, l'impegno per l'attivazione di processi di cooperazione è andato crescendo, così come si è sempre di più sentita la necessità di assegnare un preciso significato all'*enhanced cooperation* per la Internet *governance* e di definire l'uso di questa procedura per articolare le regole di gestione della Rete del futuro.

4. Prime prove di cooperazione: dal WSIS di Tunisi a oggi

Nei paragrafi 70 e 71 della Tunis Agenda si proponeva un percorso di sperimentazione composto di due fasi[10]: da una parte si prevedeva di attivare un processo di cooperazione (dall'alto verso il basso) distinto dall'Internet Governance Forum (IGF)[11] e dedicato a creare principî

[10] WSIS di Tunisi 2005 - Tunis Agenda Par. 70: "Using relevant international organizations, such cooperation should include the development of globally-applicable principles on public policy issues associated with the coordination and management of critical Internet resources. In this regard, we call upon the organizations responsible for essential tasks associated with the Internet to contribute to creating an environment that facilitates this development of public policy principles. Par. 71.: The process towards enhanced cooperation, to be started by the UN Secretary-General, involving all relevant organizations by the end of the first quarter of 2006, will involve all stakeholders in their respective roles, will proceed as quickly as possible consistent with legal process, and will be responsive to innovation. Relevant organizations should commence a process towards enhanced cooperation involving all stakeholders, proceeding as quickly as possible and responsive to innovation. The same relevant organizations shall be requested to provide annual performance reports".

[11] Vedi pargarafo 6.

applicabili globalmente; dall'altra si chiedeva alle singole organizzazioni coinvolte nel processo di creare le condizioni (dal basso verso l'alto) perché quanto al punto precedente potesse concretizzarsi. L'obiettivo di questo compromesso, sottointeso nei citati paragrafi in modo volutamente generico e quindi diversamente interpretabile, era chiaramente connesso all'attenzione politica sulla gestione del sistema di indirizzi di Internet da parte di ICANN[12]; inoltre non era chiara la lista delle organizzazioni che si riteneva dovessero essere coinvolte. I fatti che si sono succeduti hanno reso ancora più evidente come la natura dei problemi e delle soluzioni riguardanti la Internet *governance* sia articolata e basata su una pluralità di azioni di tipo diverso, difficilmente gestibili con un processo dall'alto verso il basso. Mentre, come era prevedibile, diversi processi di cooperazione si sono avviati dal basso verso l'alto quasi naturalmente, dimostrando che le organizzazioni coinvolte nella gestione della Rete non pongono barriere preconcette che possano impedire, di fatto, la costruzione di politiche pubbliche credibili e condivise. Si sono attivati diversi processi su diversi tavoli in diversi contesti, con lo scopo comune di stabilire relazioni fra tutti gli *stakeholders* della Rete ed al fine di migliorare le politiche pubbliche di Internet. Sono nati diversi processi di cooperazione fra i Governi e gli altri *stakeholders*, come non era mai accaduto prima, così come è migliorata la stessa cooperazione fra i Governi, principalmente ma non solo grazie al lavoro svolto nel GAC di ICANN e nello IGF.

5. L'evoluzione di ICANN

ICANN[13] è l'organismo di diritto privato, registrato nello Stato di California negli Stati Uniti, che sovraintende alla gestione di Internet.

[12] Vedi par. 5.

[13] L'*Internet Corporation for Assigned Names and Numbers* è un ente *no-profit*, organizzato con modalità internazionale, che ha la responsabilità di assegnare gli indirizzi IP *(Internet Protocol)* e gli identificatori di protocollo e di gestire il sistema dei nomi a dominio di primo livello (*Top-Level Domain*) nonché di curare la sicurezza e la stabilità del sistema dei *root server*. Come *partnership* pubblica-privata, ICANN ha la funzione di salvaguardare la stabilità operativa di Internet; di promuovere la competizione; di ampliare la rappresentanza delle comunità globali di Internet e di sviluppare una politica appropriata al suo intento, tramite processi partecipati e condivisi. Il processo di formulazione delle politiche, flessibile e facilmente attuabile, deriva dalle tre *Supporting Organizations*, che si occupano rispettivamente di numeri

Molti governi, non solo dei Paesi in via di sviluppo, ma anche di Paesi europei, hanno, in questi ultimi anni, posto il problema della internazionalizzazione di Internet e della legittimità internazionale dell'operato di ICANN. Recentemente con la firma della dichiarazione *Affirmation of Commitments*[14] da parte del Dipartimento del commercio del governo USA e di ICANN stessa, il processo di internazionalizzazione e democratizzazione dell'ICANN ha segnato un passo in avanti nella direzione di rendere tale organizzazione indipendente da influenze di un singolo governo.

Il fatto politico più importante è che ICANN non dovrà più riferire al governo USA[15] sul proprio funzionamento, bensì a distinti Comitati di valutazione che, in contatto con la comunità globale servita, monitoreranno ad intervalli regolari le attività svolte. ICANN, con il supporto del governo USA e nella direzione delle raccomandazioni del vertice WSIS, si è mossa per scongiurare la necessità di attivare un processo di cooperazione fra i governi dall'alto e per mettere in chiaro la posizione, anche sostenuta dall'Unione europea, contraria ad affidare il ruolo delle politiche pubbliche di Internet all'ONU ed in particolare all'ITU.

IP, *generic TLD* e *country code TLD*. Gli *Advisory Committees* e le comunità tecniche collaborano con le *Supporting Organizations* per creare politiche appropriate ed efficaci. I governi del mondo forniscono le loro raccomandazioni al *Board of Directors* attraverso un comitato consultivo governativo, il *Governmental Advisory Committee* (GAC*)*. Il Presidente di ICANN è Rod Beckstrom e il rappresentante del governo italiano è Stefano Trumpy. Vedi www.icann.org.

[14] Quando ICANN venne fondato nel 1998, si stabilì un primo *Memorandum of Understanding* (MOU o MoU) fra ICANN e il Governo USA per il coordinamento del *core* della rete Internet. La dichiarazione *Affirmation of Commitments* (AOC) firmata il 30 settembre 2009, completa una transizione iniziata 11 anni prima. La firma della dichiarazione impegna oggi ICANN a rimanere organizzazione privata *no-profit*. Dichiara che ICANN è indipendente e non controllata da alcuna entità. Impegna ICANN ad effettuare revisioni, riafferma e rinforza la funzione del *Governmental Advisory Committee,* che ha un ruolo chiave nella selezione dei componenti dei team di revisione. Il testo dell'AOC tradotto in lingua italiana è disponibile sul sito di ICANN a www.icann.org.

[15] Rod Beckstrom, Presidente e CEO di ICANN, Brussels 21 giugno 2010: "Molte persone pensano di conoscere ICANN: queste la definiscono come una organizzazione controllata dal governo USA, più interessata al proprio futuro che non aperta all'esterno e con una definita connotazione tecnica. Ma ICANN non è così oggi. In forza dell'*Affirmation of Commitments* oggi ICANN è una istituzione multinazionale che lavora per il comune obiettivo di una Internet stabile, sicura e globale. La collaborazione con il governo USA continua, ma in un contesto internazionale allargato".

6. L'evoluzione dell'Internet *Governance* Forum

L'Internet Governance Forum[16] è uno dei figli del vertice WSIS di Tunisi. È nato nel 2006 come nuovo Forum sulle questioni dell'Internet, da tenersi annualmente per un quinquennio per allargare le discussioni sulle tematiche più salienti e scottanti della Rete a tutti i potenziali gruppi d'interesse, compresi i singoli individui[17]. I Forum IGF si sono svolti nel 2006 ad *Athens*, nel 2007 a *Rio de Janeiro,* nel 2008 a *Hyderabad*, nel 2009 a *Sharm El Sheikh*. Il prossimo si terrà a *Vilnius* dal 14 al 17 settembre 2010. A quattro anni dalla partenza dell'IGF il mondo della Rete sta guadagnando una maggiore coscienza e visione globale della Internet *governance*, così come il coinvolgimento in modo paritario delle diverse organizzazioni che sono attive sugli aspetti di gestione del sistema Internet sembra sempre più vicino. L'ultimo IGF 2009 è stato quello che ha visto la partecipazione più nutrita (1800 partecipanti provenienti da 112 paesi e rappresentanti di 95 Governi) e quello dove, sul tema dell'estensione del mandato dell'IGF, si è riscontrata una sostanziale concordia. C'e tuttavia il rischio che l'IGF venga fagocitato dalla burocrazia dell'ONU di *New York*: l'IGF sta avendo un indubbio successo e quindi si moltiplicano coloro che hanno ambizioni di governarlo.

7. L'impegno dell'ONU e le posizioni delle principali organizzazioni internazionali coinvolte nella gestione delle risorse critiche di Internet

In tempi recenti, a seguito di una serie di consultazioni con i governi, il Segretario generale dell'ONU ha ritenuto più opportuno non forzare un processo di cooperazione dall'alto come inizialmente "previsto" ed ha avviato un processo per stabilire relazioni con le principali organizzazioni internazionali, le quali, come detto, avevano già iniziato a dialogare fra loro anche solo sulla spinta di provare a dare una interpretazione a cosa si volesse intendere per *enhanced cooperation*.

[16] Tutte le informazioni sui lavori dell'IGF sono disponibili sul sito ufficiale: www.intgovforum.org.

[17] La raccomandazione di creare un nuovo spazio per il dialogo per tutti gli *stakeholder* su basi di uguaglianza, a riguardo di tutte le questioni legate alla *governance* di Internet, è sempre merito dei lavori del *Working Group on Internet Governance*.

Nel 2008 il Sottosegretario generale per gli affari economici e sociali dell'ONU ha invitato alcune organizzazioni a fornire un rapporto sui passi già intrapresi nel processo di cooperazione per la politiche pubbliche di Internet e per conoscere se e come il processo di cooperazione fosse stato raggiunto.

Dieci le organizzazioni che l'ONU ha ritenuto di dover consultare:

- Internet Corporation for Assigned Names and Numbers (ICANN);
- International Telecommunication Union (ITU)[18];
- World Wide Web Consortium (W3C)[19];
- Council of Europe[20];
- Internet Society (ISOC)[21];

[18] La *International Telecommunication Union* è un'organizzazione internazionale intergovernativa all'interno dell'ONU in seno alla quale i settori pubblico e privato collaborano per lo sviluppo delle telecomunicazioni. Fondata nel 1985 è la più vecchia agenzia dell'ONU nel settore delle telecomunicazioni. Da tempo lo ITU si occupa anche dei problemi relativi ad Internet ed in particolare alla convergenza dei media. In certi campi vi è sovrapposizione di competenze tra ITU ed ICANN; tuttavia recentemente ITU ha espresso appoggio pieno al processo in corso che riguarda l'evoluzione di ICANN, ai contenuti del documento *Affirmation of Commitments* e al ruolo di ICANN come regolatore (autorità) per i numeri e nomi in Internet. Il riconoscimento del ruolo di ICANN da parte di ITU è un fatto particolarmente significativo e dovrebbe finalmente mettere a tacere le voci di persistente guerra sotterranea finalizzata a che ITU prenda il posto di ICANN sulle questioni che riguardano le politiche pubbliche nel *Domain Names System di Internet* (Vedi www.itu.int/osg/spu/intgov/).

[19] Il *World Wide Web Consortium* si occupa di standard per il *Web*; è nato nell'ottobre 1994 con Tim Berners-Lee al *Massachusetts Institute of Technology (MIT)* in collaborazione con il CERN di Ginevra. Il W3C è un consorzio internazionale di industrie oggi ospitato dal MIT negli Stati Uniti, dall'*European Research Consortium in Informatics and Mathematics* (ERCIM) in Europa e dal CNR in Italia (http://www.w3c.org).

[20] Il *Council of Europe*, con sede a Strasburgo (Francia), raggruppa oggi, con i suoi 47 Stati membri, quasi tutti i Paesi del continente europeo. Istituito il 5 maggio 1949 da 10 Stati fondatori, il Consiglio d'Europa ha come obiettivo quello di favorire la creazione di uno spazio democratico e giuridico comune in Europa, nel rispetto della Convenzione europea dei Diritti dell'Uomo e di altri testi di riferimento relativi alla tutela dell'individuo. Il Consiglio d'Europa si è espresso a favore di un impegno dei Governi e degli *stakeholders* nel processo di *enhanced cooperation* per le risorse critiche di Internet (http://www.coe.int/).

[21] La *Internet Society* è al centro dei dibattiti internazionali sull'organizzazione della gestione della Rete sin dagli inizi degli anni '90 ed oggi partecipa con impegno al processo di definizione della *governance* della Rete. ISOC è sede organizzativa dell'*Internet Engineering Task Force* (IETF), l'organismo che definisce gli standard tecnici ed operativi della Rete. Il CNR è socio fondatore di *Internet Society* dal '92. Sul sito di ISOC Italia è disponibile un'ampia documentazione sui temi della *governance* della Rete e sui relativi processi in corso. Vedi www.isoc.org e www.isoc.it.

- Organization for Economic Cooperation and Development (OECD)[22];
- United Nations Educational, Scientific and Cultural Organization (UNESCO)[23];
- World Intellectual Property Organization (WIPO)[24];

Number Resource Organization (NRO)[25];

Internet Engineering Task Force (IETF).

Inizialmente solo il *Council of Europe*, ICANN, ISOC, ITU, OECD e il W3C hanno dato risposta. Successivamente il 19 febbraio 2010, tutte le dieci istituzioni, di nuovo sollecitate dalla *Commission on Science and Technology for Development*[26], hanno fornito i loro aggiornamenti. Tutti i

[22] L'*Organisation for Economic Co-operation and Development* è un'organizzazione internazionale di studi economici per i 31 paesi membri ed ha sede a Parigi. L'organizzazione svolge prevalentemente un ruolo di assemblea consultativa che consente un'occasione di confronto delle esperienze politiche, per la risoluzione dei problemi comuni, l'identificazione di pratiche commerciali ed il coordinamento delle politiche locali ed internazionali dei paesi membri. Con la *Seoul Declaration for the Future of Internet Economy,* l'OECD si è espresso sui valori e i principî base che guidano lo sviluppo della *Internet Economy*. Vedi www.oecd.org.

[23] L'UNESCO è l'organizzazione dell'ONU fondata a Parigi il 16 novembre 1945. Più di 180 Paesi ne sono membri. Nel dicembre del 2009 l'UNESCO ha siglato un accordo con ICANN per aiutare la diffusione degli IDN (*Internationalised Domain Names*) che sono un significativo strumento per superare la diversità linguistica in Internet. Vedi www.unesco.org.

[24] Il *World Intellectual Property Organization* si occupa dal 1970 dei problemi della proprietà intellettuale nel mondo. È una organizzazione internazionale che opera come agenzia speciale dell'ONU, deputata all'amministrazione dei trattati internazionali e ad assistere i Governi, le organizzazioni ed il settore privato nell'affrontare le problematiche in materia di proprietà intellettuale. WIPO è attiva sui temi della *governance* di Internet fin dal primo WSIS del 2003. Vedi www.wipo.org.

[25] La *Number Resources Organization* è stata creata dai "RIRs - *Regional Internet Registries*" per formalizzare i loro sforzi cooperativi. È nata per gestire l'insieme delle risorse IP non ancora assegnate del "Number Resource pool", per promuovere il processo *bottom-up* dello sviluppo delle *policy* e per fungere da punto di raccolta per i suggerimenti della comunità Internet, all'interno del sistema dei RIRs. Opera anche come *Address Supporting Organization* di ICANN. Vedi www.nro.org.

[26] La *Commission on Science and Technology for Development* (CSTD) è uno strumento di supporto del *EConomic and SOcial Council* dell'ONU. Dal 1992 la Commissione è chiamata a fornire raccomandazioni all'Assemblea generale dell'ONU derivanti dall'impatto delle questioni di innovazione scientifica e tecnologica sullo sviluppo sociale. I temi della Internet *governance* fanno parte dell'agenda di questa commissione.

contributi ricevuti sono pubblicati e disponibili in Rete[27]. Al momento l'ONU si è riservato aggiornamenti in merito da mettere in agenda per la sessantaseiesima Assemblea generale che si terrà nel 2011.

8. Conclusioni

In sostanza l'ONU ha dilazionato l'impostazione di un eventuale processo di cooperazione dall'alto verso il basso come era previsto nel vertice WSIS del 2005, mentre ICANN e lo IGF sono diventati i luoghi ove primariamente si verificano i progressi di cooperazione e collaborazione, ed in molti sono favorevoli a che la *enhanced cooperation,* opportunamente definita, diventi un *modus operandi* comune a tutte le organizzazioni che sovraintendono al funzionamento di Internet. Dunque quanto auspicato nel WSIS di Tunisi si può ritenere che sia stato raggiunto: importanti progressi sono avvenuti e abbiamo posto le basi per migliorarli in futuro con meccanismi *multistakeholder* sempre più forti e con una maggiore apertura delle organizzazioni internazionali che hanno influenza nelle decisioni sulla Internet *governance*.

Verso coloro che si ostinano a vedere la *enhanced cooperation* come un processo distinto da ICANN e da IGF, vi è la preoccupazione che essi tendano a voler creare un'altra organizzazione intergovernativa *ad hoc* per la gestione del sistema Internet, come accadde a suo tempo per i sistemi di telecomunicazione precedenti. Ci riferiamo alle reti telefoniche e televisive che sono figlie di pianificazioni e investimenti centralizzati e controllati attraverso vecchi modelli iper-regolamentati, certamente inapplicabili e dannosi per il sistema Internet. Al contrario infatti, la rete Internet è nata dal basso come interconnessione di infrastrutture, di risorse informative e di contenuti, messi in comune dagli utenti stessi. Su Internet, gli utenti sono costantemente liberi di inserire in rete nuovi contenuti, nuovi servizi, e persino nuove tecnologie; da questa spinta, anziché da pianificazioni e investimenti centralizzati, sono nate tutte le tecnologie fondamentali della rete, incluso il World Wide Web[28].

[27] Rif. E/2009/92/CRP1, *United Nations*, *Commission on Science and Technology for Development*, 18 maggio 2010, *Enhanced Cooperation on Public Policy Issues Pertaining to the Internet.*

[28] V. Bertola, *op. cit.*

Il futuro della Internet *governance* non può essere determinato esclusivamente dalla legge dei governi, diversamente si tratta di convenire su poche, semplici, linee guida, da declinare poi in precetti e regolamenti[29]; il sistema Internet è nei fatti un fenomeno globale risultato della somma di diversi interessi locali, l'unico modo per gestirlo è quello di andare oltre gli irrigidimenti di alcuni governi, rafforzando il dialogo *multistakeholder* e favorendo nuove forme di *enahanced cooperation*, per istradare nella stessa direzione la molteplicità di interessi presenti nel sistema Internet.

[29] J. MARINO, *Futuro della gestione internazionale di Internet*, Quaderno edito da ISOC Italia, agosto 2005 (www.quadernionline.it).

L'Internet *Governance* tra tecnica, politica e diritto

DAVIDE DE GRAZIA*

1. PREMESSA

Pochi fattori hanno contribuito come l'avvento della comunicazione via Internet a quella "intensificazione di relazioni sociali mondiali che collegano tra loro località distanti, facendo sì che gli eventi locali vengano modellati dagli eventi che si verificano a migliaia di chilometri di distanza e viceversa"[1], cui si fa sintetico riferimento con l'espressione "globalizzazione".

La comunicazione telematica ha avuto importanti conseguenze di ordine sociale, culturale ed economico, modificando profondamente lo stile di vita e di lavoro degli abitanti del pianeta e creando i presupposti per l'allargamento del raggio di azione delle grandi imprese commerciali e l'intensificazione degli scambi transfrontalieri[2]. Si tratta di processi di cambiamento connotati da spiccata intersettorialità, che toccano la dimensione economico-finanziaria, ma anche quella ambientale, culturale, politico-militare, sociale, psicologica, senza dimenticare le implicazioni sui flussi migratori e sulle dinamiche dei rapporti interetnici[3].

Tutti questi fenomeni sono stati accompagnati, ed anzi amplificati, dalla diffusione dei mezzi di comunicazione di massa, e in particolare della rete Internet, che non a torto è da molti considerata il "catalizzatore essenziale della globalizzazione contemporanea"[4].

* L'Autore è dottore di ricerca in Diritto pubblico e assegnista di ricerca in Diritto amministrativo presso il Dipartimento di Diritto pubblico "A. Orsi Battaglini" dell'Università di Firenze. È inoltre professore a contratto di Diritto amministrativo presso la Libera Università di Bolzano.

[1] A. GIDDENS, *Le conseguenze della modernità*, Bologna, Il Mulino, 1994, p. 71.

[2] J.-B. AUBY, *La globalisation, le droit et l'État*, Parigi, Montchrestien, 2003, pp. 13 e ss.

[3] U. ALLEGRETTI, *Diritti e Stato nella mondializzazione*, Troina, Città aperta, 2002, pp. 18 e ss.

[4] J. GOLDSMITH, T. WU, *Who Controls the Internet? Illusions of a Borderless World*, New York, Oxford University Press, 2006, p. 179.

Si tratta di un fenomeno che suscita l'interesse del giurista soprattutto per la vocazione originaria della Rete a costituire oggetto di un regime globale, rispetto al quale il diritto è chiamato alla elaborazione di soluzioni istituzionali capaci di governare processi di questa dimensione.

Da diverse parti si è ritenuto che proprio la comunicazione via Internet costituisca uno dei settori in cui sta avverandosi la previsione della emersione del "diritto amministrativo globale"[5]. L'organizzazione che detiene i più significativi poteri relativi alla gestione delle risorse critiche di Internet e alla regolazione dei servizi di accesso alla Rete, l'Internet Corporation for Assigned Names and Numbers (ICANN), è stata annoverata tra le amministrazioni globali[6], pur se con la precisazione, non di poco conto, che si tratterebbe di un organismo di amministrazione globale interno a uno Stato (gli Usa), anzi interno ad uno Stato (la California) membro di uno Stato federale, per di più costituito come ente di diritto privato[7].

Lo spazio a disposizione impone di contenere la trattazione ad alcuni soltanto dei molti problemi legati al governo di Internet[8]. Ci si limiterà dunque fare il punto sullo stato attuale della gestione della "infrastruttura logica" di Internet, costituita dall'insieme delle risorse di identificazio-

[5] L'emersione del diritto amministrativo globale è stata descritta per la prima volta da B. KINGSBURY, N. KRISCH, R.B. STEWART, *The Emergence of Global Administrative Law*, in "Law and Contemporary Problems", 2005, 15, pp. 68 e ss. Tra gli studi in lingua italiana possono segnalarsi R.B. STEWART, *Il diritto amministrativo globale*, in "Rivista trimestrale di diritto pubblico", 2005, pp. 633 e ss.; S. CASSESE, *Il diritto amministrativo globale. Una introduzione*, in "Rivista trimestrale di diritto pubblico", 2005, pp. 331 e ss.; S. BATTINI, *Organizzazioni internazionali e soggetti privati: verso un diritto amministrativo globale?*, in "Rivista trimestrale di diritto pubblico", 2005, pp. 359 e ss.; S. CASSESE, *Gamberetti, tartarughe e procedure. Standards globali per i diritti amministrativi nazionali*, in "Rivista trimestrale di diritto pubblico", 2004, pp. 657 e ss.; S. BATTINI, *Amministrazioni senza Stato. Profili di diritto amministrativo internazionale*, Milano, Giuffrè, 2003.

[6] B. CAROTTI, *L'ICANN e la governance di Internet*, in "Rivista trimestrale di diritto pubblico", 2007, pp. 683 e ss.; S. CASSESE, *Oltre lo Stato*, Roma, Laterza, 2006, pp. 15 e ss. e p. 44.

[7] Cfr. G. FALCON, *Ordine giuridico e ordine politico nel diritto amministrativo globale*, in Carta P., Cortese F. (a cura di), "Ordine giuridico e ordine politico: esperienze, lessico, prospettive", Padova, Cedam, 2008, pp. 174 e ss.

[8] Per una più diffusa ed approfondita trattazione dei diversi profili dell'*Internet Governance* sia consentito il rinvio a D. DE GRAZIA, *Il governo di Internet*, Milano, FrancoAngeli, 2010, in corso di pubblicazione.

ne che, rendendo i terminali e le reti reciprocamente interoperabili, permettono la comunicazione via Internet.

Della importanza e della complessità di questi temi si sono per primi resi conto gli autori statunitensi, che hanno dedicato approfondite riflessioni al problema della stessa suscettibilità alla regolazione di una rete di telecomunicazioni globale rispetto alla quale i confini tra gli Stati tendono ad essere irrilevanti[9]. Nel dibattito europeo il tema è divenuto di attualità con notevole ritardo rispetto al Nord America[10].

2. L'INTERNET *GOVERNANCE*

Dopo diversi decenni di generale disinteresse, durante i quali la lotta per la conquista del controllo sulle risorse critiche della Rete ha visto schierati soltanto pochi contendenti consapevoli del loro carattere strategico per lo sviluppo della comunicazione via Internet, il tema è finalmente entrato nel dibattito pubblico internazionale a partire dal 2007, quan-

[9] La letteratura statunitense comincia ad assumere proporzioni notevoli. Per limitarsi ad alcuni dei contributi più significativi, possono vedersi: D.W. DREZNER, *The Global Governance of the Internet: Bringing the State Back In*, in "Political Science Quarterly", 2004, Vol. 119, n. 3, pp. 477 e ss.; J. GOLDSMITH, T. WU, *Who Controls the Internet? Illusions of a Borderless World*, cit.; D.R. JOHNSON, D.G. POST, *Law and Borders: the Rise of Law in Cyberspace*, in "Stanford Law Review", 1996, Vol. 48, n. 5, pp. 1367 e ss.; B. KAHIN, J.H. KELLER (eds.), *Coordinating the Internet*, Cambridge, MA, 2000, II ed.; M.A. LEMLEY, *Place and Cyberspace*, in "California Law Review", 2003, Vol. 91, pp. 521 e ss.; L. LESSIG, *Code 2.0*, New York, Basic Books, 2006; M.L. MUELLER, *Ruling the Root. Internet Governance and the Taming of Cyberspace*, Cambridge, Ma., MIT Press, 2002; H.H. PERRITT JR., *Cyberspace and State Sovereignty*, in "Journal of International Legal Studies", 1997, n. 3, pp. 155 e ss.; A. THIERER, C.W. CREWS (eds.), *Who Rules the Net? Internet Governance and Jurisdiction*, Washington, Cato Institute, 2003; T. WU, *Cyberspace Sovereignty? – The Internet and the International System*, in "Harvard Journal of Law and Technology", 1997, Vol. 10, n. 3, pp. 648 e ss.

[10] Si vedano gli scritti di S. MUÑOZ MACHADO, *La regulación de la red*, Madrid, Taurus, 2000; P. AMBLARD, *Regulation de l'internet: l'elaboration des regles de conduit par le dialogue internormatif*, Bruxelles, Bruylant, 2004; E. CLERC, *La gestion semi-priveé de l'Internet*, in Morand C.-A. (ed.), *Le droit saisi par la mondialisation*, Bruxelles, Bruylant, 2001, pp. 333 e ss.; J.-B. AUBY, *La globalisation, le droit et l'État*, cit., pp. 34 e ss.; L. KOLETSOU, K. KOMAITIS, E. MAGANARIS, *The Role of ICANN in Internet Governance: Friend or Foe?*, in "European Review of Public Law", 2006, Vol. 18, n. 4, pp. 1346 e ss.; G.L. CONTI, *La governance della rete*, in AA.VV., *Lo Stato costituzionale: la dimensione nazionale e la prospettiva internazionale. Scritti in onore di Enzo Cheli*, Bologna, Il Mulino, 2010, in corso di pubblicazione.

do è stato inserito ufficialmente nell'ordine del giorno dell'Internet Governance Forum di Rio de Janeiro. Il dibattito sviluppatosi in quella sede ha permesso di evidenziare l'emersione di due ordini di problemi.

In primo luogo, il nuovo interesse degli Stati per la gestione delle risorse critiche di Internet. Questa attenzione accomuna regioni già tecnologicamente avanzate (il Giappone, l'Unione europea) e Paesi appartenenti alle aree in via di sviluppo (l'Africa, l'America Latina, l'Asia), che vedono nella Rete una importante leva per la promozione dello sviluppo economico, delle relazioni internazionali, dei rapporti commerciali e finanziari.

La percezione delle risorse critiche di Internet come un "collo di bottiglia" da superare per l'accesso alle risorse messe a disposizione dal nuovo mezzo di comunicazione globale è alla base dell'istanza, che trova sempre sostenitori nei dibattiti e nei *forum* internazionali, per il superamento dell'approccio unilaterale al controllo della radice di Internet finora mantenuto attraverso l'asse tra il governo degli Stati Uniti e l'ICANN[11].

In secondo luogo, il problema della qualificazione delle funzioni di gestione delle risorse critiche di Internet come meramente tecniche ovvero implicanti scelte e valutazioni di carattere politico.

Non di rado gli attori impegnati, a vario titolo, nell'esercizio di queste funzioni utilizzano l'argomento della natura meramente tecnica dell'attività di coordinamento e di gestione delle risorse di identificazione della rete Internet, allo scopo di contrastare i tentativi, più o meno compiuti, di ricondurre l'esercizio di tali funzioni in una qualche sede politicamente legittimata[12].

Questa impostazione è stata criticata dalla dottrina statunitense, che ha osservato come l'atteggiamento da sempre mantenuto dai soggetti che si sono nel tempo avvicendati nel controllo della radice logica di Internet è

[11] Cfr. Second Meeting of the Internet Governance Forum (IGF), Rio de Janeiro, 12-15 novembre 2007, Chairman's Summary, disponibile al sito http://www.intgovforum.org/Rio_Meeting/Chairman Summary.FINAL.16.11.2007.pdf, pp. 2 e ss.

[12] Cfr., ad es., E. Dyson, *Response to Ralph Nader's Questions*, 15 giugno 1999, in http://www.icann.org/correspondence/dyson-response-to-nader-15jun99.htm, in cui l'allora presidente del Board of Directors dell'Icann, in risposta alle sollecitazioni provenienti da Ralph Nader, precisa che "ICANN does not 'aspire to address' any Internet governance issues; in effect, it governs the plumbing, not the people. It has a very limited mandate to administer certain (largely technical) aspects of the Internet infrastructure in general and the Domain Name System in particular".

stato generalmente dovuto ad una sorta di "allergia" al metodo democratico da parte di questa *élite* tecnocratica[13].

Il rilievo politico, e non meramente tecnico, delle questioni sottese alla gestione della infrastruttura logica di Internet, costituita dalle risorse di identificazione della Rete (IP e DNS), emerge sotto diversi punti di vista, sui quali è opportuno soffermarsi sinteticamente.

3. La radice logica di Internet come infrastruttura essenziale

La "radice logica" è data dall'insieme delle risorse numeriche ed alfanumeriche che, consentendo l'identificazione univoca dei terminali e delle reti interconnessi, permettono il corretto instradamento dei dati veicolati lungo la Rete. La gestione della radice così definita costituisce il cuore stesso di Internet, perché presso di essa sono allocate le funzioni relative alla definizione delle caratteristiche dello spazio dei nomi (*namespace*) e della relativa estensione (mediante la determinazione del numero dei nomi di dominio di primo livello generici e geografici), nonché alla delega delle attività di registrazione dei nomi di dominio di secondo livello e di tenuta dei relativi registri. Alla radice della Rete possono però essere ricondotte anche le funzioni di assegnazione ed allocazione degli indirizzi numerici costituiti dal protocollo IP, senza i quali l'utente non potrebbe essere "riconosciuto" dal sistema di instradamento automatico dei pacchetti e dunque non potrebbe connettersi a Internet[14].

La radice logica costituisce una infrastruttura essenziale, la cui disponibilità condiziona la possibilità di esercitare attività economiche (si pensi alle attività di prestazione dei diversi servizi di connessione, registrazione, *hosting* e così via), ma anche diritti e libertà fondamentali come la manifestazione del pensiero, l'informazione, l'associazione, il culto, etc.

La caratterizzazione della radice "ufficiale" come *essential facility* discende dalla impossibilità della sua duplicazione[15].

[13] M.L. Mueller, *Ruling the Root*, cit., pp. 93 e ss.

[14] Riconducono alla radice di Internet il sistema degli indirizzi IP M.L. Mueller, *Ruling the Root*, cit., pp. 5 e ss. e J. Goldsmith, T. Wu, *Who Controls the Internet?*, cit., pp. 30 e ss.

[15] Sulle condizioni che devono sussistere perché una determinata infrastruttura possa considerarsi *essential facility*, con conseguente imposizione in capo al suo detentore degli

La duplicazione della radice, infatti, è impedita non già da ragioni tecniche, ma da motivi politici ed economici.

Se infatti da un punto di vista strettamente tecnico non ci sarebbero particolari ostacoli alla possibilità della duplicazione della rete logica, dal momento che la maggiore o minore scarsità delle risorse disponibili dipende unicamente dalla capacità dei protocolli di identificazione scelti di creare "spazi" dei nomi o dei numeri più o meno "estesi", il discorso cambia radicalmente affrontando il problema dal punto di vista della convenienza economica e della opportunità politica di una tale operazione.

Dal punto di vista economico, la possibilità della creazione di "radici alternative" (*alternative roots*) è fortemente disincentivata dalle esternalità che caratterizzano le attività di fornitura di servizi di comunicazione in rete a causa dei fenomeni di *feedback*: il valore che ciascun utente assegna alla opportunità di connettersi alla rete dipende dal numero delle altre persone che già vi fanno parte e, dunque, "a parità di altre condizioni, è meglio essere connessi a una rete di grandi dimensioni piuttosto che a una rete piccola"[16].

Questa osservazione, che può apparire ovvia, è densa di ripercussioni rispetto all'adozione delle scelte strategiche da parte degli operatori del mercato e spiega, in termini economici, gli insuccessi dei tentativi di creazione e di diffusione di reti alternative alla "radice ufficiale".

Da questa constatazione discende inoltre, dal punto di vista politico, la non desiderabilità della paventata "balcanizzazione della Rete" in vista del miglior perseguimento dell'interesse generale alla diffusione, alla funzionalità e alla universalità del servizio di telecomunicazione[17].

obblighi di contrarre stabiliti dall'art. 82 TrCE (oggi art. 102 TFUE) per le imprese in posizione dominante cfr. CGCE, sez. VI, 26.11.1998, C-7/97, *Oscar Bronner*, in *Racc.*, 1998, I, pp. 7791 e ss., punto 44. Per un articolato commento alla decisione v. D. DURANTE, G.G. MOGLIA, A. NICITA, *La nozione di essential facility tra regolazione e antitrust. La costruzione di un test*, in "Mercato, concorrenza e regole", 2001, 2, pp. 257 e ss.

16 C. SHAPIRO, H.R. VARIAN, *Information Rules. Le regole dell'economia dell'informazione*, Milano, Etas, 1999, pp. 213 e ss.

17 Le ragioni della inopportunità della proliferazione delle radici alternative sono riassunte nella Rfc 2826 del 2000 (intitolata *IAB Technical Comment on the Unique DNS Root* e disponibile in http://www.ietf.org/rfc/rfc2826.txt) secondo cui "to remain a global network, the Internet requires the existence of a globally public name space (…) derived from a single, globally unique root. (…) That one root must be supported by a set of coordinated root servers administered by a unique naming authority".

L'essenzialità della infrastruttura logica ai fini della fornitura e della fruizione di servizi di comunicazione via Internet implica tutta una serie di conseguenze in ordine al particolare regime della rete logica, e degli atti attraverso i quali si realizza la sua gestione, in vista del perseguimento di obiettivi quali l'accesso degli operatori economici alla rete ai fini della fornitura dei servizi, l'accesso degli utenti ai servizi di connessione e così via.

Come noto, problemi come quelli appena accennati si pongono al centro dei processi di liberalizzazione dei servizi di pubblica utilità nei settori caratterizzati dalla presenza di reti non duplicabili, nei quali l'affermazione della competizione concorrenziale tra i fornitori di servizi all'utenza finale viene perseguita essenzialmente attraverso la disaggregazione della filiera produttiva del servizio, prima verticalmente integrata in capo ad un unico operatore economico, e la realizzazione di un mercato concorrenziale a valle della rete infrastrutturale, con mantenimento della gestione di quest'ultima nelle mani di un operatore (cui eventualmente può essere inibita la possibilità di competere nel mercato dei fornitori del servizio all'utenza finale) tenuto a rendere l'infrastruttura disponibile agli erogatori del servizio[18].

Se si considera poi l'analogia della funzione svolta dalle risorse numeriche ed alfanumeriche di identificazione dei terminali connessi alla rete Internet con quella propria delle numerazioni telefoniche (anch'esse deputate al corretto instradamento del flusso di dati in cui si risolve la comunicazione tra due utenti), non può non osservarsi come nei Paesi che hanno compiuto la scelta della liberalizzazione dei relativi servizi, e che quindi hanno visto l'ingresso nel mercato di operatori privati dal lato dell'offerta dei servizi di telefonia, la tendenza costante è stata quella di mantenere in mano pubblica il controllo della numerazione, considerata "risorsa nazionale"[19] e affidata il più delle volte alla gestione di amministrazioni pubbliche di regolazione[20].

[18] Cfr. F. TRIMARCHI BANFI, *Lezioni di diritto pubblico dell'economia*, Torino, Giappichelli, 2009, II ed., *passim*.

[19] In questo senso si veda l'art. 15 del Codice delle comunicazioni elettroniche (d.lgs. n. 259/2003).

[20] M.L. MUELLER, *Ruling the Root*, cit., p. 26; International Telecommunication Union, *Trends in Telecommunication Reform: Convergence and Regulation*, Ginevra, 1999.

Esigenze di segno analogo presiedono al mantenimento in un'unica istanza, oggettivamente amministrativa, delle funzioni di gestione delle risorse critiche di identificazione che permettono il corretto funzionamento della rete Internet.

4. La gestione della radice attuata dall'ICANN

4.1. La natura politico-amministrativa delle decisioni dell'ICANN

A svolgere le funzioni di gestione della radice logica di Internet è, come si è accennato nel paragrafo introduttivo, l'Internet Corporation for Assigned Names and Numbers (ICANN).

Le competenze dell'ICANN sono indicate nell'art. I del suo statuto[21], che definisce la missione della *corporation*. Secondo la sezione 1, l'ICANN è chiamata a coordinare la gestione dei sistemi globali di identificazione nell'ambito della rete Internet e garantire il funzionamento dei sistemi di identificazione unica di Internet, assicurandone la stabilità e la sicurezza.

Lo stesso statuto indica, nella sezione 2 dell'art. I, i valori fondamentali (*core values*) che l'ICANN assume quali principî-guida della sua azione e dunque gli interessi generali che la *corporation* si impegna a curare nell'espletamento della sua missione[22]. Si tratta di interessi di grande rilievo e il fatto che lo statuto li richiami esplicitamente quali principî-guida dell'azione della *corporation* appare di indubbio significato al fine della qualificazione della natura dell'attività dell'ICANN, che non si limita evidentemente ad una mera gestione tecnica.

[21] *Bylaws for Internet Corporation for Assigned Names and Numbers*, testo disponibile in http://www.icann.org/general/bylaws.htm.

[22] Tali valori sono, in sintesi, quelli della stabilità, sicurezza e interoperabilità globale della Rete; della innovazione e della diffusione delle informazioni; del decentramento, ove possibile ed opportuno, delle funzioni di coordinamento e di indirizzo presso organismi rappresentativi degli interessi coinvolti; della promozione della partecipazione delle diverse realtà geografiche e culturali interessate; della promozione di un ambiente competitivo, in particolare, ove possibile e rispondente all'interesse pubblico, rispetto alle attività di registrazione dei nomi di dominio; della trasparenza, obiettività, neutralità, integrità, correttezza e tempestività dei processi decisionali; della responsabilità (*accountability*) nei confronti della "*Internet community*"; del riconoscimento del ruolo dei governi nazionali e delle autorità pubbliche, pur mantenendo il radicamento nel settore privato delle funzioni di gestione della Rete.

Appare infatti assai difficile ritenere che la missione dell'ICANN possa essere adempiuta mediante un mero "coordinamento tecnico" della gestione delle risorse di identificazione. L'adempimento della missione indicata nello statuto richiede invece la soluzione di questioni "politiche", attraverso l'attenta (e discrezionale) ponderazione di interessi.

Si pensi ad esempio al riferimento alla promozione della concorrenza, con particolare riguardo al mercato dei servizi di registrazione dei nomi di dominio, e all'incidenza su tale materia delle decisioni rimesse all'ICANN in materia di creazione di nuovi nomi di dominio di primo livello, di definizione delle politiche di risoluzione dei conflitti relativi a marchi e nomi di dominio e di accreditamento dei *registrar*[23].

Si consideri inoltre che lo stesso statuto riconosce che i *core values* sono elencati nella sezione 2 dell'art. I in termini volutamente assai generici e ciò per consentire all'ICANN di adattarli alle situazioni di fatto, nella consapevolezza che possono verificarsi circostanze che non permettono di rimanere pienamente fedeli a tutti i principî indicati: in tali circostanze, lo statuto rimette all'apprezzamento dell'ICANN la selezione degli interessi in concreto più rilevanti e il bilanciamento tra valori e interessi tra loro confliggenti[24].

Nel prevedere la necessità di tale bilanciamento, lo statuto non fa che riconoscere l'intrinseca discrezionalità (politico-amministrativa, si direbbe) dei poteri dell'ICANN, che devono essere esercitati mediante l'apprezzamento e la ponderazione della concreta consistenza degli interessi in gioco, ossia attraverso "una comparazione qualitativa e quantitativa degli interessi pubblici e privati che concorrono in una situazione sociale

[23] E. CLERC, *La gestion semi-privée de l'Internet*, cit., pp. 342 e ss., che qualifica la missione di Icann al riguardo come "tecnico-politica".

[24] Cfr. l'ultimo paragrafo dell'art. I, sez. 2, secondo cui "these core values are deliberately expressed in very general terms, so that they may provide useful and relevant guidance in the broadest possible range of circumstances. Because they are not narrowly prescriptive, the specific way in which they apply, individually and collectively, to each new situation will necessarily depend on many factors that cannot be fully anticipated or enumerated; and because they are statements of principle rather than practice, situations will inevitably arise in which perfect fidelity to all eleven core values simultaneously is not possible. Any ICANN body making a recommendation or decision shall exercise its judgment to determine which core values are most relevant and how they apply to the specific circumstances of the case at hand, and to determine, if necessary, an appropriate and defensible balance among competing values".

oggettiva, in modo che ciascuno di essi venga soddisfatto secondo il valore che l'autorità ritiene abbia nella fattispecie"[25].

Si tratta dunque di ponderare, bilanciare e operare scelte tra "valori fondamentali" non sempre facilmente armonizzabili e tra interessi individuali e collettivi diversi e potenzialmente conflittuali in vista della definizione dell'interesse pubblico (in concreto). Un potere, questo, che negli ordinamenti nazionali viene normalmente riconosciuto all'amministrazione pubblica in quanto inserita nel circuito dell'indirizzo politico che costituisce il veicolo per la legittimazione del potere di fare questo tipo di scelte[26].

Nel caso dell'ICANN, la selezione e la ponderazione dei diversi interessi avviene in seno al suo organo di vertice, il Board of Directors. Nella retorica che normalmente avvolge la descrizione delle funzioni della *corporation*, la ragione del radicamento in capo al *board* del potere di scegliere viene rinvenuta nel fatto che nell'organo si realizzerebbe un processo *bottom-up*, e dunque il pieno coinvolgimento di tutte le istanze interessate nel governo della Rete, secondo una logica *multistakeholder*.

Scostato il velo della suggestione, però, ci si avvede che gli interessi coinvolti nella gestione delle risorse critiche non trovano affatto adeguata e paritaria rappresentazione nei meccanismi decisionali della *corporation*. Il processo di nomina dei componenti del *board* è congegnato per assicurare maggior peso decisionale ad alcuni soltanto dei portatori di interessi (riuniti nelle tre *supporting organizations*), mentre per altre istanze la rappresentatività in seno all'organo dell'ICANN è solo indiretta ed eventuale[27].

Le stesse organizzazioni di supporto hanno l'iniziativa rispetto all'adozione di qualsiasi decisione relativa alle *policies* concernenti la gestione delle risorse critiche di Internet.

Dovrebbe apparire chiaro che la composizione del *board* secondo il modello della rappresentanza organica degli interessi non risponde affatto alla logica dell'*expertise*, che sarebbe coerente con una funzione della *corpo-*

[25] In questo consiste, appunto, la discrezionalità politico-amministrativa: cfr. M.S. GIANNINI, *Il potere discrezionale della pubblica amministrazione*, Milano, Giuffrè, 1939, pp. 74 e ss. V. anche M.S. GIANNINI, *Diritto amministrativo*, Vol. II, Milano, Giuffrè, 1993, III ed., pp. 45 e ss.; D. SORACE, *Diritto delle amministrazioni pubbliche*, Bologna, Il Mulino, 2007, IV ed., pp. 271 e ss.

[26] D. SORACE, *Diritto delle amministrazioni pubbliche*, cit., pp. 19 e ss., pp. 265 e ss.

[27] Cfr. art. VI dello statuto dell'Icann.

ration limitata al mero coordinamento tecnico delle risorse di identificazione. Di più: il differente "peso" attribuito ai diversi *stakeholders* in sede di nomina dei membri del *board* e all'interno dei processi decisionali, lungi dal caratterizzare in senso tecnico le funzioni dell'organo, esprime esso stesso una chiara opzione "politica" di favore verso certi interessi rispetto ad altri.

Tutto ciò senza contare il fortissimo rischio di "cattura del regolatore" cui è sottoposta l'ICANN per effetto del diretto coinvolgimento nei processi decisionali dei portatori degli interessi toccati dagli atti relativi alla gestione della radice[28].

La suggestione alimentata dall'affermazione della natura meramente tecnica delle funzioni svolte mira a nascondere la loro vera sostanza e a sottrarre il loro esercizio ai circuiti della legittimazione politico-democratica, perpetrando l'influenza dominante di alcuni centri di interesse economico.

A smentire ulteriormente la tesi del rilievo meramente tecnico delle funzioni dell'ICANN milita anche il coinvolgimento dei governi nazionali nelle questioni relative alla gestione della radice.

Tale coinvolgimento trova un momento significativo di manifestazione nell'attività del Governmental Advisory Committee (Gac), istituito il 2 marzo 1999 con il compito di fungere da elemento di raccordo tra l'ICANN e i governi nazionali. Nelle intenzioni dell'amministrazione statunitense e del primo Board of Directors, l'istituzione del comitato doveva servire a tacitare le pretese dei governi, i quali avrebbero avuto così l'illusione di disporre di uno strumento per partecipare all'attività dell'ICANN senza però acquisire un peso sostanziale nei processi decisionali[29].

[28] Cfr. E. CLERC, *La gestion semi-privée de l'Internet*, cit., pp. 353 e ss. Sulla teoria della cattura del regolatore cfr. G.F. STIGLER, *The Theory of Economic Regulation*, in "Bell Journal of Economics and Management Science", 1971, n. 2, pp. 3 e ss.; S. PELTZMAN, *Toward More General Theory of Regulation*, in "Journal of Law and Economics", 1976, n. 19, pp. 211 e ss.; S. PELTZMAN, *The Economic Theory of Regulation after a Decade of Deregulation*, in Baldwin R., Scott C., Hood C. (eds.), "A Reader on Regulation", Oxford, Oxford University Press, 1998, pp. 93 e ss.; T. MAKKAI, J. BRAITHWAITE, *In and Out the Revolving Doors: Making Sense of Regulatory Capture*, *ibidem*, pp. 173 e ss.; J.Q. WILSON, *The Politics of Regulation*, New York, Basic Books, 1980, pp. IX e ss.

[29] Cfr. M.L. MUELLER, *Governments and Country Names: ICANN's Transformation into an Intergovernmental Regime*, testo disponibile alla pagina http://faculty.ischool.syr.edu/mueller//gacnames.pdf, p. 5, secondo il quale "the Americans who dominated ICANN's

Nonostante queste premesse, il Gac ha acquistato nei fatti un rilevante peso nella elaborazione delle *policies* dell'ICANN[30], peso che ha trovato infine formale riconoscimento nello statuto della *corporation*, ai sensi del quale il Board of Directors deve tenere nella dovuta considerazione, tanto in sede di formulazione quanto di adozione delle *policies*, il parere espresso dal comitato e, qualora si determini a discostarsi dallo stesso, è tenuto a informare il comitato delle relative ragioni. In questo caso il Gac e il *board* sono obbligati a cercare insieme una composizione reciprocamente accettabile dell'*impasse*[31]. Solo se i due organi non riescono a trovare una soluzione, il *board* può procedere nella adozione della decisione, motivando circa il mancato recepimento del parere del Gac, senza pregiudizio per i diritti e gli obblighi dei componenti del comitato in relazione alle materie rientranti nelle loro responsabilità[32].

*4.2. La relazione tra l'*ICANN *e il governo statunitense*

L'ICANN esercita le funzioni sopra accennate in virtù dell'autorità che le deriva da due gruppi di accordi che legano la *corporation* all'amministrazione statunitense.

Un primo gruppo di accordi concerne lo svolgimento, da parte dell'ICANN, delle funzioni di coordinamento e di gestione del sistema dei nomi di dominio (DNS), in vista del perseguimento degli obiettivi della promozione della concorrenza nei segmenti di mercato relativi alle attività legate al sistema dei nomi di dominio e della possibilità di scelta degli utenti, della crescita della fiducia di questi ultimi, del mantenimento della sicurezza, della stabilità e della capacità del sistema di resistere agli attacchi esterni e adattarsi continuamente e del miglioramento dei processi decisionali in chiave di trasparenza ed *accountability*.

management and interim Board initially viewed GAC as a prophylactic that did as much to keep government out of ICANN's affairs as it did to bring them in".

[30] M.L. MUELLER, *Don't Like the UN? How About GAC?*, 17 agosto 2005, in http://www.icannwatch.org/article.pl?sid=05/08/17/1653243.

[31] Art. XI, sez. 2(1)(j), dello statuto.

[32] Art. XI, sez. 2(1)(k). In argomento cfr. L. KOLETSOU, K. KOMAITIS, E. MAGANARIS, *The Role of ICANN in Internet Governance: Friend or Foe?*, cit., pp. 1330 e ss.; B. CAROTTI, *L'ICANN e la governance di Internet*, cit., pp. 698 e ss.

I rapporti tra ICANN e governo statunitense rispetto allo svolgimento di queste funzioni hanno conosciuto nel tempo una significativa evoluzione, segnata dai diversi *Memorandum of Understanding* sottoscritti dalle parti dal 1998 al 2003 e poi dal *Joint Project Agreement* del 2006[33] e, da ultimo, dalla *Affirmation of Commitments* del 2009[34]. Questa evoluzione è stata caratterizzata dalla progressiva emancipazione dell'ICANN, nello svolgimento delle funzioni oggetto degli accordi, dalla "tutela" del Dipartimento del commercio americano[35]. Il controllo governativo in precedenza si concretava in un sostanziale potere di veto sulle decisioni relative alla introduzione di nuovi nomi di dominio generici di primo livello, al trattamento dei dati personali raccolti in occasione della fornitura dei servizi di registrazione, alle relazioni con i gestori dei registri dei nomi di dominio geografici di primo livello[36]. Era inoltre previsto l'obbligo dell'ICANN di presentare alla controparte pubblica rapporti periodici sull'attività svolta[37]. La *Affirmation of Commitments* non contempla più obblighi di questo genere in capo alla *corporation*: l'amministrazione americana rinuncia ad esercitare questa supervisione, sostituita dalla previsione di un processo di revisione triennale dell'attività della *corporation* nell'ambito di specifiche aree tematiche, e si impegna a partecipare all'attività dell'ICANN quale componente del Governmental Advisory Committee[38].

[33] Il JPA è disponibile all'indirizzo http://www.icann.org/general/JPA-29sep06.pdf.

[34] La *Affirmation of Committments* si legge alla pagina http://www.icann.org/en/announcements/announcement-30sep09-en.htm.

[35] Il processo, che avrebbe dovuto completarsi alla scadenza del primo *Memorandum of Understanding*, aveva subìto diverse battute d'arresto a causa dei contrasti in seno al Dipartimento del commercio circa l'opportunità di un arretramento del governo rispetto alla gestione delle risorse di identificazione, contrasti che spiegano le ragioni dei numerosi rinnovi del MoU e la sottoscrizione, solo nel 2006, di un accordo di transizione come il *Joint Project Agreement*: cfr. L. KOLETSOU, K. KOMAITIS, E. MAGANARIS, *The Role of ICANN in Internet Governance: Friend or Foe?*, cit., pp. 1346 e ss.

[36] M.L. MUELLER, H. KLEIN, J. HOFMANN, L. MCKNIGHT, D.L. COGBURN, *Political Oversight of ICANN: A Briefing for the WSIS Summit*, 1° novembre 2005, in http://www.internetgovernance.org/pdf/political-oversight.pdf, pp. 3 e ss.

[37] Cfr. punto V, lett. B, n. 8, del *Memorandum of Understanding* del 1998, cit.; art. II, lett. C, n. 2, del *Joint Project Agreement*, cit., che aveva sostituito i *report* semestrali che l'Icann era tenuta a inviare al Dipartimento del commercio sotto i precedenti MoU, con la pubblicazione di un rapporto annuale.

[38] *Affirmation of Commitments*, cit., punto n. 6.

L'entusiasmo suscitato dalla sottoscrizione della *Affirmation of Commitments*[39] non tiene nella dovuta considerazione la circostanza che il controllo effettivo del sistema dei nomi di dominio è garantito all'ICANN dall'altro gruppo di accordi cui si faceva riferimento, relativi allo svolgimento delle funzioni originariamente esercitate dalla Iana (c.d. *Iana functions*).

Si tratta innanzitutto del coordinamento della gestione della radice del DNS, onde garantire la manutenzione e l'aggiornamento continuo delle banche dati contenute nei *server* radice (*root server*). Tali operazioni consistono nel materiale aggiornamento giornaliero dei tredici *root server*, necessario per permettere il corretto funzionamento della funzione di risoluzione dei nomi[40]. Rientrano poi nelle *Iana functions* svolte dall'ICANN anche gli adempimenti tecnici necessari per la ridelegazione dei registri per i nomi di dominio di primo livello, generici e geografici[41]. Infine, ICANN svolge la fondamentale *Iana function* consistente nella ripartizione dei blocchi di indirizzi IP tra i Regional Internet Registries (Rir), i quali poi provvedono a distribuire gli indirizzi, in blocchi più piccoli, ai Local Internet Registries (Lir) che li allocano agli ISP associati perché siano assegnati agli utenti finali dei servizi di connessione alla Rete.

L'autorità dell'ICANN nell'esercizio di queste funzioni deriva dal c.d. *Iana contract* stipulato tra la *corporation* e il governo statunitense nel

[39] Cfr. ad es. il documento della Commissione europea intitolato *La Commissione europea si compiace per l'iniziativa degli Stati Uniti verso una gestione di Internet più indipendente, più responsabile e più internazionale*, Bruxelles, 30 settembre 2009, in http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1397&format=HTML&aged=0&language=IT&guiLanguage=en). Gli stessi toni entusiastici avevano in precedenza salutato la sottoscrizione del *Joint Project Agreement*.

[40] Per quanto riguarda il *root server* A, ovvero il *server* autorevole dei nomi radice, l'aggiornamento è sotto la diretta responsabilità dell'Icann, che ha contrattualmente affidato la relativa attività alla società californiana VeriSign. Gli altri dodici *server* radice sono gestiti da operatori diversi dall'Icann o da suoi *contractors*: ai fini del coordinamento di cui si è detto, la *corporation* è chiamata a stipulare accordi con ciascuno di tali operatori.

[41] Per questi ultimi, Iana/Icann ha elaborato un documento intitolato *Understanding the ccTLD Delegation and Redelegation Procedure*, emendato nel 2007 e disponibile alla pagina http://www.iana.org/domains/root/delegation-guide, che, tra le altre cose, prevede l'approvazione del Dipartimento del commercio statunitense prima che la delegazione al nuovo operatore nazionale di registro abbia effetto.

2000[42], che attribuisce alla prima il potere di gestire risorse (quali sono le risorse di identificazione nella rete Internet) che altrimenti non rientrerebbero nella sua disponibilità, fornendo così la "leva" fondamentale per regolare efficacemente i mercati dei servizi di connessione a Internet.

Il rapporto tra ICANN e governo statunitense relativo all'esercizio delle *Iana functions* non ha subìto alcuna modifica per effetto dalla stipulazione della *Affirmation of Commitments*. Queste funzioni continuano ad essere esercitate dalla *corporation* in virtù dello *Iana contract*, che conferisce al governo statunitense un "potere di vita o di morte" sulla autorità dell'ICANN sulla radice di Internet[43]. Essendo immutato il fondamento del conferimento di queste funzioni, il controllo ultimo sulla radice di Internet è dunque conservato dal governo statunitense[44], il quale, per questa via, mantiene un forte potere di condizionamento dello svolgimento, da parte dell'ICANN, dell'attività di regolazione che forma oggetto della *Affirmation of Commitments*.

Gli stessi accordi relativi alla gestione del DNS (dai *Memorandum* alla *Affirmation*), inoltre, hanno sempre preveduto espressamente per ciascuna

[42] *Contract Between ICANN and the United States Government for Performance of the IANA Functions*, sottoscritto il 9 febbraio 2000 (al sito http://www.icann.org/general/iana-contract-09feb00.htm) e rinnovato il 14 agosto 2006 (il testo aggiornato è consultabile alla pagina http://www.icann.org/general/iana-contract-14aug06.pdf).

[43] Cfr. M.L. MUELLER, *Taking a Hard Look at the "Affirmation"*, 30 settembre 2009, in http://blog.internetgovernance.org/blog/_archives/2009/9/30/4337767.html, il quale osserva che "the IANA contract, which still gives the U.S. a unilateral, life-or-death power over Icann's authority over the DNS root zone file, is unchanged by [the Affirmation of Commitments]".

[44] Cfr. al riguardo A.M. FROOMKIN, *Wrong Turn in Cyberspace: Using ICANN to Route around the APA and the Constitution*, in "Duke Law Journal", 2000, Vol. 50, n. 1, pp. 125 e ss. In una ipotetica situazione di emergenza, dunque, il governo potrebbe ritenere opportuno riappropriarsi del diretto controllo della radice della Rete e recedere dallo *Iana contract*. Si noti che in passato si è già avuta una chiara manifestazione della autorità ultima del governo in tema di gestione delle risorse costituenti la radice di Internet. Ci si riferisce all'episodio che vide protagonisti Ira Magaziner, in rappresentanza del governo, e Jon Postel. Il 28 gennaio 1998 quest'ultimo tentò di "dirottare" la funzione di risoluzione autorevole dei nomi di dominio dal *name server* "uffiicale" presso la Network Solutions al *server* dei nomi gestito dalla Iana presso l'ISI diretto dallo stesso Postel. Il tentativo fu prontamente bloccato da Magaziner con la minaccia di pesanti conseguenze. L'episodio è narrato in J. GOLDSMITH, T. WU, *Who Controls the Internet?*, cit., pp. 43 e ss. e in M.L. MUELLER, *Ruling the Root*, cit., p. 162.

delle parti la facoltà del recesso anticipato, condizionata alla sola comunicazione scritta da darsi con preavviso di almeno centoventi giorni[45]. Evidentemente, una previsione del genere risulta difficilmente armonizzabile con l'idea del definitivo trasferimento al "*private sector*" (ovvero all'ICANN) di quelle funzioni di regolazione economica che presuppongono l'abilitazione alla gestione delle risorse costituenti la radice della Rete.

Il quadro appena tratteggiato induce a ritenere che, a dispetto della suggestione alimentata dalla rinuncia del governo statunitense alle proprie prerogative per diventare uno dei tanti componenti del Governmental Advisory Committee, la capacità dell'amministrazione americana di influenzare le scelte dell'ICANN risulta tuttora molto forte.

5. Conclusioni: Internet e la *rule of law*

I problemi che si sono molto sinteticamente evidenziati nei paragrafi che precedono richiedono uno sforzo di concettualizzazione del fenomeno del governo della Rete che ancora non risulta essere stato compiuto nelle sedi appropriate.

In particolare, è mancata fino ad oggi una riflessione approfondita sulla fisionomia che dovrebbe assumere la gestione delle risorse critiche della Rete e la regolazione delle attività da esse dipendenti una volta superata la contingente "emergenza" rappresentata dalla necessità di realizzare un apparato tecnico-organizzativo in grado di accompagnare i primi stadi della costruzione e della diffusione di Internet.

I tempi sono maturi perché la gestione della Rete sia finalmente informata al rispetto di un principio di legalità o di una *rule of law*[46].

La scala globale delle funzioni (e dei poteri) dell'ICANN pone la questione, finora inedita, della legittimazione (e della responsabilità, innanzitutto politica), in mancanza di un quadro pattizio che dia fondamento a livello internazionale all'attribuzione delle funzioni di cui si discute, di un

[45] Cfr. *Memorandum of Understanding*, art. VII; *Joint Project Agreement*, art. III, lett. C; *Affirmation of Commitments*, punto n. 11.

[46] H. Klein, *ICANN Reform: Establishing the Rule of Law*, aprile 2005, in http://www.internetgovernance.org/pdf/ICANN-Reform-Establishing-the-Rule-of-Law.pdf. Sulla "*rule of law* globale" si veda anche L. Torchia, *Lezioni di diritto amministrativo progredito*, Bologna, Il Mulino, 2010, pp. 28 e ss.

ente a porre in essere atti (sostanzialmente amministrativi) efficaci nei confronti di soggetti posti al di fuori dell'ordinamento cui l'ente appartiene.

Il problema non è solo teorico. Già oggi l'ICANN dispone, in virtù dell'autorità conferitale, come si è visto, dagli atti siglati con il governo statunitense, di significativi poteri di incisione unilaterale dei diritti e delle libertà che nella rete Internet possono trovare un veicolo di espressione e di esercizio, il ricorso ai quali può essere utilizzato su scala globale come strumento di dissuasione o di repressione di comportamenti non desiderati nei confronti di individui, enti o interi Paesi, che potrebbero vedere limitata la fruibilità delle risorse di identificazione e dunque la possibilità di connettersi alla Rete e la stessa "*Internet membership*"[47].

Di fronte a questo potere dai caratteri del tutto inediti, l'esigenza di un principio regolatore e di adeguate istanze di tutela, capaci di assicurare protezione contro gli abusi, appare ormai ineludibile.

Obiettivi come quelli adesso tratteggiati richiederebbero che del problema del governo della Rete si sentisse pienamente investita la comunità internazionale e che al *deficit* di legittimazione democratica del governo della radice di Internet su scala globale si ponesse rimedio attraverso il ricorso agli strumenti propri della cooperazione intergovernativa. Un processo di questo genere incontrerebbe le intuibili resistenze dei soggetti che fino ad oggi, più o meno manifestamente, hanno detenuto il controllo della radice, ma varrebbe a sanare il *vulnus* costituito dalla assenza di una *rule of law* quale principio informatore delle funzioni di gestione della Rete.

[47] J. GOLDSMITH, T. WU, *Who Controls the Internet?*, cit., p. 32.

Libertà e regolazione in Internet. A proposito della *Governance*

ANTONIO A. MARTINO*

> *The end of law is not to abolish or restrain, but to preserve and enlarge freedom. For in all the states of created beings, capable of laws, where there is no law there is no freedom. For liberty is to be free from restraint and violence from others, which cannot be where there is no law; and is not, as we are told, a liberty for every man to do what he lists. For who could be free, when every other man's humor might domineer over him? But a liberty to dispose and order freely as he lists his person, actions, possessions, and his whole property within the allowance of those laws under which he is, and therein not to be subject to the arbitrary will of another, but freely follow his own.*
>
> John Locke, Civil Government

1. INTRODUZIONE

Dice Montesquieu nell'*Esprit de Lois* che i commercianti, che sono vili per condizione, sono pure disonesti, quando la legge non riconosce per tempo i loro diritti.

Noi ci troviamo in un momento particolare nel quale l'irruenza di Internet nella nostra vita è cosi possente e così totalizzante, che dobbiamo affrettarci a darci delle regole per non soccombere alla mancanza di libertà, come bene diceva Locke.

Per carità, non vogliamo cadere nell'ingenuità che nel secolo scorso ha fatto pensare a più d'uno che, cambiando le leggi, sarebbe cambiata la società. È la società, invece, che ha bisogno di leggi.

Crediamo, infatti, che prima ci debba essere l'esperienza sociale, e poi le leggi, non il contrario. Il fatto è che queste leggi non devono essere troppo tardive, per non comprimere i diritti di libertà.

* L'Autore è direttore del Master in Scienza della legislazione presso la Universidad del Salvador (Argentina) in collaborazione con l'Università di Pisa, nonché direttore scientifico della Scuola di alti studi per il Mercosur presso la Universidad de la Repubblica (Montevideo) in collaborazione con la Regione Toscana e l'Università di Pisa.

Lo scopo di questo lavoro è mostrare che solo dentro le regole si può attuare la libertà, e che questa regolazione dovrebbe essere la più universale possibile, data la natura dell'oggetto regolato (senza dimenticare i contesti sociali e politici), e dovrebbe contenere il minor numero di regole possibile. La legislazione, infatti, deve essere avara di parole[1].

Allo stesso tempo, però, occorre affrontare con urgenza il tema della regolazione del governo di Internet.

Internet è un oggetto complesso, quindi va trattato con le metodologie che studiano, descrivono e prescrivono che cosa è un oggetto complesso e come funziona (e come potrebbe funzionare meglio).

Nel 2015 tre miliardi e mezzo di persone - la metà del genere umano - avranno accesso ad Internet. Non si è mai verificata una tale rivoluzione in tema di libertà di espressione e di comunicazione. Ma come sarà questo nuovo mezzo? Quali nuove distorsioni e quali ostacoli troveranno i nemici di Internet[2].

La natura di Internet impone anche che queste leggi siano le più generali possibili, somigliando ad una specie di *jus gentium* moderno ed attuale. Ma poche norme, in tempi di corruzione, possono generare più norme[3], e, come diceva Montesquieu, "Le leggi inutili servono a indebolire quelle necessarie".

Internet – che è una rete di reti – è entrato ormai in ogni parte dalla nostra vita. Attraverso tale mezzo possiamo richiedere un certificato di nascita o di matrimonio, conoscere i risultati della carriera scolastica di nostro figlio, conseguire la patente di guida, effettuare la dichiarazione dei redditi, avviare attività commerciali, prenotare visite culturali, … e possiamo ovviamente richiedere anche il certificato di morte altrui. Infinite sono, dunque, le ricadute positive di Internet, tanto per gli individui, quanto per le imprese.

Ovviamente, le problematiche sollevate dall'impiego di Internet sono diverse a seconda che si consideri il settore pubblico o quello privato, che

[1] Vedi A.A. MARTINO, *Algunas consideraciones sobre el Manual del Digesto Argentino*, 1999, in http://www.antonioanselmomartino.it/.

[2] Così si è espresso Bernard Kouchner, Ministro francese degli Affari esteri ed europei. Cfr. http://www.isoc.it/index.php?option=com_content&task=view&id=688&Itemid=21.

[3] V. Étienne Bonnot De Condillac.

si operi, ad esempio, in una organizzazione non governativa (ONG) e in una impresa di profitto.

Ciò richiede un coinvolgimento di tutti gli specialisti giuridici, pubblicisti e privatisti, perché le questioni da affrontare investono trasversalmente i più diversi settori del diritto tradizionalmente intesi (v. per esempio la tematica della protezione del consumatore in Internet).

Di fronte a quest'onnipresenza e trasversalità del mezzo, è necessario tenere alta la bandiera dei diritti, poiché essa può essere facilmente travolta.

Noi crediamo, infatti, che i "diritti" non siano entità a sé, ma siano invece elementi di un sistema che ne riconosce sì l'esistenza, ma che, allo stesso tempo, li limita, ponendo obblighi; diversamente, la nozione di diritto sarebbe un *flatus vocis*.

Riteniamo quindi necessaria una "dichiarazione generale dei diritti in Internet", che gradualmente sia accettata da tutti i Paesi, o almeno dalla maggioranza, diventando per via consensuale obbligatoria: una sorta di *Bill of Rights* di Internet.

Lo scopo del presente lavoro è per l'appunto quello di dimostrare che si può presentare Internet come un sistema unitario, nel quale la *governance* ed il governo costituiscono aspetti della stessa medaglia.

2. Il governo di Internet

In una precedente pubblicazione mi sono occupato della *governance* di Internet, introducendo innanzitutto un chiarimento che ritengo importante quando si ragiona del tema in oggetto. Riporto qui di seguito testualmente il mio pensiero: "In materia politologica si fa una netta differenza nella letteratura dominante – che è angloamericana – tra "governo", "governabilità" e "*governance*". La prima parola in italiano vuol dire troppe cose, ma in generale in qualsiasi lingua la nozione di governo può essere riferita all'organizzazione dello Stato che nelle costituzioni è parte ineludibile.

La governabilità è relativa alla durata dei governi (sopratutto nei sistemi parlamentari) e in particolare alla possibilità di governare anche in situazioni di minoranza parlamentare. Questo vuol dire che i partiti politici e gli attori politici trovano più importante far funzionare un governo – anche in minoranza –, così rafforzando il sistema politico, piuttosto che metterlo in crisi per tentare di andare loro al governo, indebolendo il sistema politico. Gli esempi in Italia sono numerosi.

La *governance* invece consiste in tutte le azioni che le pubbliche amministrazioni ritengono necessarie per indurre cittadini e imprese a perseguire i propri fini istituzionali. Quindi la *governance* è positiva – come la governabilità –, e si verifica, in particolare, quando queste azioni amministrative tendono alla semplificazione e alla qualità, per esempio rendendo più facile, più accessibile, più trasparente e più rapido ottenere un'informazione, richiedere certificati, autorizzazioni e, sopratutto, interagire con la pubblica amministrazione. Con questo significato il termine *governance* senza dubbio riecheggia alcune espressioni ancora in uso in Toscana quali "rigovernare la tavola", "rigovernare la casa", e persino "il fattore è andato a governare i buoi"[4].

Questa volta però, pur senza rinunciare alla *governance*, vorrei concentrarmi più sul governo di Internet e sulla sua regolazione giuridica.

Considerandolo un oggetto complesso, vedremo Internet come un sistema unico, vale a dire come un oggetto che nasce, ha una fase di sviluppo e poi muore. Non che io stia predicendo la morte di Internet, al contrario, ma vederlo in questo modo nella sua complessità ci consentirà di capire, da un lato, cosa lo tiene insieme e, dall'altro, cosa minaccia la sua vita.

Se Internet è un sistema, necessariamente presenta i seguenti elementi/caratteri:

- la descrizione della composizione (C), dell'ambiente (E), della struttura (S) e del meccanismo (M) del sistema;
- l'adattamento, che è determinato dal rapporto del sistema con l'ambiente esterno, all'interno del quale si trova e con il quale, a sua volta, interagisce;
- il perseguimento degli obiettivi cui il sistema è preposto, mediante la mobilitazione delle energie necessarie;
- l'integrazione, che è definita dalle azioni che aiutano a mantenere la coerenza del sistema.

A proposito della composizione di Internet, possiamo osservare che esso si compone per l'appunto: *a)* di una rete globale di reti di computer; e *b)* dell'insieme delle risorse presenti su ciascun computer, che risultano accessibili per mezzo dei collegamenti esistenti tra le diverse reti.

[4] A.A. MARTINO, *Premessa*, in Martino A.A., "Aspetti giuridici di Internet. Contributo ai lavori dell'Internet Governance Forum", n. spec. di "Quaderni dell'Internet italiano", 2007, *on-line* all'indirizzo http://www.quadernionline.it/igf_2007/indice.html.

Quando un computer si collega a Internet, un *software* particolare presente in esso "inganna" Internet, facendogli accettare il computer come se fosse una parte delle reti che compongono Internet stesso. In tal modo il singolo computer dell'utente diviene letteralmente parte di Internet.

Ad un livello intermedio, la rete Internet può invece essere vista anche come una vasta raccolta di grandi librerie di informazioni, tutte disponibili in linea per potervi fare ricerche o per essere prelevate ed utilizzate[5].

Con riguardo all'ambiente di Internet, possiamo notare che esso copre praticamente tutta la Terra, ovviamente non in modo omogeneo: vi è, infatti, una densità maggiore di Internet nell'emisfero nord ed in particolare negli Stati Uniti e nel Canada. Lo spazio di Internet non è un altrove. Al contrario, esso rappresenta una delle tante tessere del complesso *puzzle* in cui ci troviamo a vivere: un *environment* complicato, abitato da comunità che vivono a velocità diverse, in cui i flussi d'informazione s'intrecciano con quelli di merci e persone, in cui alto e basso, globale e locale, *naïveté* e *hi-tech* si scontrano tra loro.

In tale contesto, il *digital divide* è uno dei problemi maggiori legati alle nuove tecnologie e ad Internet, una criticità molto sottile, che non fa clamore, ma che tuttavia preclude molte possibilità di sviluppo alla maggior parte dei Paesi del mondo. Con il termine *digital divide,* infatti, s'intende proprio il divario tecnologico o di competenza che impedisce a grandi fette della popolazione mondiale di poter accedere a Internet. È un problema che riguarda qualsiasi Paese, anche se è particolarmente accentuato nei Paesi del terzo mondo ed in quelli in via di sviluppo. Non bisogna comunque dimenticare che il *digital divide* incide pesantemente anche nei paesi industrializzati, nei quali vige la cosiddetta *Network Society:* anche nella nostra Italia, fanalino di coda in Europa per l'utilizzo di Internet.

[5] L'inglese Wellington Grey si è preso la briga di classificare il *web* usando uno schema familiare: la tavola degli elementi. La classificazione di Wellingtong è piuttosto divertente. Al posto di gas, metalli e non metalli, nelle colonne sono indicati – per raggruppamento – motori di ricerca, internet tool, aggregatori, sistemi di produttività. Al posto dell'originale H (idrogeno) c'è l'elemento Y!; al posto dell'elio (He) c'è Wikipedia; al posto del litio (Li) c'è Google, e via così. Ogni casella ha la sigla, la URL e il ranking (sarà di pagine viste?) che consentono facili riferimenti tra i siti.

Non va dimenticato poi che esiste anche un ambiente esterno ad Internet, che ne influenza lo sviluppo, che si compone di sottosistemi molto complessi quali le società, le economie, la cultura, il sistema normativo.

La struttura di Internet (S) è una ragnatela di calcolatori connessi in miriadi di reti, all'interno dei quali le informazioni sono concentrate in terminali chiamati *host*, con dei protocolli per avere accesso agli indirizzi TCP/IP.

Ma parlare della struttura di Internet significa anche parlare del modo in cui esso è organizzato e governato, attraverso l'ICANN (*Internet Corporation for Assigned Names and Numbers*), che provvede alle definizione degli standard tecnici e delle diverse norme giuridiche, l'ISOC (*Internet Society*) e le organizzazioni ad essa connesse - tra le quali lo IETF (*Internet Engineering Task Force*), che sviluppa gli standard di Internet-, il W3C (*World Wide Web Consortium)* che sovrintende allo sviluppo della tecnologia WWW, le entità intergovernative come lo ITU (*International Telecommunications Unit*) delle Nazioni Unite, il WIPO (*World Intellectual Property Organisation*) ed altre. Tutte queste istituzioni/organizzazioni collaborano tra loro per una evoluzione di Internet basata sul contributo paritario di tutti gli Stati nella gestione del sistema degli indirizzi di Internet. Come si può vedere, non esiste, dunque, un ente unico preposto al governo della Rete. Quest'oggetto complesso, infatti, pur presentando il carattere degli organismi internazionali, si deve tuttavia adattare alle normative nazionali, non esistendo ad oggi un soggetto sovranazionale regolatore preminente.

Con riguardo al meccanismo (M) del sistema Internet, si può notare che esso cresce ed è accresciuto in ragione delle pratiche oggettive che emergono in ogni parte del mondo, e che fanno di Internet uno strumento variegato e, per ora, pieno di sorprese e risorse per compiere tutte le azioni umane, trattandosi di un enorme contenitore di conoscenza: sulla scienza, sull'arte, sul commercio, sul turismo, sul governo elettronico (vale a dire sulla funzione concreta di *governance*), sulla nascita e sugli altri eventi della vita di persone ed imprese. Per dirla in latino: "H*omo sum; humani nihil a me alienum puto*"[6].

[6] "Sono uomo, niente di quello che è umano mi è alieno". Ovviamente, non pretendo di dare dell'uomo a Internet; adatterei, tuttavia, tale espressione in tal modo: "Sono un prodotto umano e niente che agli uomini concerne (dal punto di vista della conoscenza) mi è alieno".

La modalità di Internet riguarda le prassi mediante le quali effettivamente si praticano le connessioni ad Internet, gli usi che si fanno dei dati, il modo di condividerli, le regole di funzionamento in parte dettate dalla stessa prassi, sempre più attraverso l'ICANN e gli altri enti sopra richiamati.

L'adattamento attiene al rapporto del sistema con l'ambiente esterno, all'interno del quale Internet si trova e con il quale, a sua volta, interagisce. Come ogni sistema, Internet, infatti, è autopoietico[7], ma deve anche avere rapporti con l'ambiente esterno, sotto il profilo economico, culturale, storico, sociale. Se è vero che Internet sta via via sostituendo i preesistenti mezzi che consentivano di acquisire notizie, dati scientifici e conoscenze più in generale, è anche vero però che il suo grado di utilità dipende dallo sviluppo tecnologico della regione considerata, variando esso a seconda dell'età degli utenti, del mezzo sociale e dalla situazione economica. Questo rapporto con l'esterno è, dunque, biunivoco: Internet è sì condizionato dall'ambiente esterno, ma allo stesso tempo esso contribuisce al cambiamento dell'ambiente in cui opera.

Quando si parla del perseguimento degli obiettivi ci si riferisce, come sopra anticipato, alla mobilitazione delle energie del sistema Internet verso gli obiettivi prefissati. L'obiettivo principe di Internet è funzionare sempre e funzionare ovunque. Non importa quante sfide esso debba affrontare e quante difficoltà interne incontri, in ragione del fatto che ogni partecipante ad esso ha scopi e finalità diversi (basti penare alle aziende produttrici di *hardware* o di *software*, agli amministratori di reti, agli utenti, ai governi nazionali, ecc.).

L'integrazione del sistema Internet è realizzata da tutte quelle azioni che sono finalizzate al mantenimento della coerenza del sistema stesso, e che quindi consistono nella determinazione di standard tecnologici

[7] Il termine "autopoiesi" è stato coniato nel 1972 da Humberto Maturana a partire dalla parola greca *auto*, ovvero *se stesso*, e *poiesis*, ovverosia *creazione*. In pratica un sistema autopoietico è un sistema che ridefinisce continuamente se stesso ed al proprio interno si sostiene e si riproduce. Un sistema autopoietico può quindi essere rappresentato come una rete di processi di creazione, trasformazione e distruzione di componenti che, interagendo fra loro, sostengono e rigenerano in continuazione lo stesso sistema. Inoltre, il sistema si *autodefinisce*, di fatto, ovvero il dominio di esistenza di un sistema autopoietico coincide con il dominio topologico delle sue componenti.

condivisibili, ma anche di regole comuni giuridiche e politiche, che permettano la libera circolazione dell'informazione e l'accesso ad Internet per la maggior parte delle persone e delle istituzioni. In questo particolare momento storico proprio gli standard e le regole comuni sono in pericolo: sia perché alcuni governi limitano o si propongono di limitare la libera circolazione delle informazioni in Internet; sia perché alcune imprese si servono di questo mezzo per offendere, confondere e frodare; sia, infine, perché un mezzo così potente sveglia i più ambiziosi sogni di potere.

3. I CASI LIMITE

Di fronte al dilagare di Internet ed alle malefatte compiute attraverso tale mezzo, alcuni osservatori sostengono che è giunto il momento di imbavagliare la Rete. Intendiamoci: coloro che sostengono che Internet è pericoloso hanno ragione. Anzi, personalmente ritengo addirittura che la maggiore o minore importanza di una determinata scoperta, o di un fenomeno, possa essere valutata proprio in termini di maggiore o minore pericolosità della stessa o dello stesso. Non a caso, i due fenomeni più eclatanti che faranno ricordare il ventesimo secolo sono la fusione dell'atomo ed Internet, entrambi ritenuti estremamente pericolosi, ma, al contempo, estremamente interessanti e forieri di conseguenze per la nostra vita sul pianeta Terra.

I possibili rischi derivanti da un cattivo uso dell'energia atomica sono attualmente monitorati dalla comunità internazionale e da un apposito Comitato sulla sicurezza atomica, che ha sede a Vienna[8].

Ancora non esiste un analogo Comitato che controlli le attività dannose commesse mediante Internet, ma potrebbe essere istituito, se si avessero idee chiare sui compiti da attribuirgli. Il fatto che Internet sia adoperato per le efferatezze più disprezzabili dal punto di vista etico non è conseguenza della tecnologia, ma dell'agire umano. Internet è un mezzo, e come tale notoriamente con esso si possono perseguire i fini più nobili, come quelli più perversi. Spetta quindi a noi giuristi la riflessione su come affrontare i problemi che l'impiego di questo mezzo può generare.

[8] IAEA (International Atomic Energy Agency). Cfr. www.iaea.org.

In generale, la mia convinzione è che ciascuna branca del diritto possiede già tutti gli elementi per regolare l'uso di questo meraviglioso strumento, adattando ad esso le regole esistenti. Non escludo, tuttavia, che possa risultare necessario un ordinamento speciale; ma su tale argomento sarei davvero molto cauto[9].

Ad esempio, tra le diverse perversioni che si stanno diffondendo in Internet, ce n'è una denominata W*ar Porn*, che esprime un certo tipo di voyerismo, esibendo non necessariamente fatti di guerra, ma certamente elementi catastrofici di morte e sangue, che possono accadere anche in guerra. Il termine *porn*, peraltro, non sta a significare "pornografico", ma indica semplicemente l'efferatezza delle mostruosità che l'uomo può compiere più o meno intenzionalmente[10].

Altro esempio è quello della cosiddetta *culture of humiliation o* cultura dell'umiliazione. In questo caso il gioco consiste nell'assistere al massacro quasi certamente di una fattissima Whitney Houston, che continua a fare concerti, ma non riesce a finire una canzone (il video in cui biascica disperatamente "I Will Always Love You" è stato molto condiviso).

E ancora, sono stati fondati gruppi contro Mario Balotelli, intemperante giocatore dell'Inter, e i titoli di tali gruppi sono irriferibili.

Sono forse riferibili, ma a dir poco avvilenti, i nomi dei gruppi ignoti e terrificanti che se la prendono con amici (insomma, amici) e compagni di scuola. Un esempio: "Per quelli che pensano che Cislaghi puzzi". Sembra innocente, ma se Cislaghi è in terza media, una cattiveria del genere diffusa *on-line* gli segnerà la vita.

[9] Non vorrei, infatti, che accadesse come in Argentina, dove è stata approvata una nuova legge per la protezione di genere (femminile), la quale in realtà non fa altro che riprendere tutte le norme esistenti, riunendole in una nuova legge speciale. Simili operazioni sono pericolose, perché potrebbero indurre il legislatore a moltiplicare le leggi speciali a seconda delle idee che ha sulla divisione del mondo: leggi sulle macchine, leggi sui pelati, ecc.

[10] Il caso più eclatante è quello di un video che riprende le forze armate americane in Irak, in cui si vede una macchina piuttosto capiente che potrebbe contenere dei terroristi. La macchina è, in realtà, una normalissima berlina sulla quale vengono trasportati civili e giornalisti, ma ciononostante – ed è questa la parte "porn" del video – i piloti degli elicotteri chiedono impazientiti di essere autorizzati a sparare e, dopo aver sparato, commentano finalmente il massacro compiuto.

In America, il *mobbing* via Facebook ha già provocato dei suicidi tra gli adolescenti. C'è chi obietta che i suicidi ci sono sempre stati, tra i ragazzi marginalizzati e derisi. C'è però anche chi sostiene che oggi il rischio è maggiore, grazie all'anonimato possibile sul *web*. È noto, infatti, che – ad esempio – su Facebook ci si può dare un'identità fittizia, farsi degli amici, ma anche distruggere qualcuno a furia di post e foto. "Non bisogna più guardare l'altro negli occhi per insultarlo", ha detto al WSJ Parry Aftab, avvocato esperto in cyber-sicurezza. "Siamo tutti coraggiosi, alla tastiera. Ed è più facile attraversare il confine tra umorismo e crudeltà". Più facile anche a causa del bombardamento dei *reality*. "A furia di vedere gente che si rende ridicola e si fa umiliare per aumentare l'audience, molti pensano sia normale"[11].

Il 30 aprile 2010 circa tremila studenti liceali marinarono la scuola e si riunirono nella piazza Indipendenza della città di Mendoza in Argentina. Ovviamente questo non poteva accadere senza Internet, anzi senza una rete sociale quale Facebook, ma vogliamo censurare Internet per evitare le "marinate" collettive?

O vogliamo fare come in Cina dove Internet è sottoposto a verifiche automatiche ossessive. Spesso peraltro tali controlli degenerano nella comicità, innescata dagli equivoci di caratteri linguistici consonanti. "Carota" è un termine bloccato: il primo ideogramma, infatti, coincide con il nome del presidente Hu Jintao. Con la bomba atomica di Internet, seguita dai missili dei *social network* e dei motori di ricerca, la Cina si è vista costretta a erigere la nuova "Grande muraglia di fuoco" contro l'invasione delle idee dall'Occidente e l'evasione dei cervelli dall'Oriente. L'ufficio della propaganda è stato superato dal Gapp, la "General Administration of Press and Publication", a cui sono affidate la gestione e la supervisione dei media. Quattordici ministeri si contendono l'obbedienza di oltre due milioni di funzionari che battono il cyberspazio per "armonizzare le informazioni" e "guidare l'orientamento dell'opinione pubblica". Ma questo supera il tema Internet per sfociare in un comportamento politico dittatoriale.

Nonostante tale dispiegamento di mezzi censori, non si è potuto evitare che il 20 maggio di quest'anno il Dalai Lama, che da gennaio ha un

[11] M.L. Rodotà, in "La Repubblica", 7 maggio 2010.

account su Twitter, chattasse con i cinesi che hanno sistemi di *proxy* e filtri che consentono di aggirare gli sbarramenti della censura, collegandosi a server domiciliati all'estero, attraverso un interprete che traduceva le risposte del Dalai Lama dal tibetano in mandarino.

4. La legislazione

Come è stato notato, "In senso stretto di *governance*, la rete dipende dai protocolli TCP/IP e dalla gestione degli indirizzi. Gli attori principali sono la Internet Corporation for Assigned Names and Numbers (ICANN), la Internet Society (ISOC), l'Internet Engineering Task Force (IETF), il World Wide Web Consortium (W3C) e l'International Telecommunication Union (ITU). Intorno a questi attori e ai rappresentanti dei governi nazionali ruota la possibilità di intervenire per fissare i criteri che consentano a Internet di funzionare, attraverso la migliore collaborazione degli enti citati. In senso largo di *governance* il sistema Internet ha a che fare con tutti i problemi etici, politici, giuridici ed economici connessi ai contenuti veicolati dalla rete, che sono affrontati a livello locale dagli stati nazionali, e a livello globale attraverso strutture sopranazionali, o direttamente attraverso trattati; sono incluse tutte le questioni di politica pubblica che hanno necessità di essere coordinate globalmente come la libertà di espressione in rete, l'accesso alla rete, il rispetto delle diversità e la sicurezza per superare i problemi sociali connessi agli utilizzi non appropriati della rete"[12].

Un'organizzazione importante in questo contesto è dunque l'ICANN, un organismo californiano pubblico-privato, che opera di concerto con il Ministero del commercio degli Stati Uniti, assolvendo ad una numerosa serie di compiti. Tra questi:

- il coordinamento della cessione dei parametri di protocollo tecnico;
- lo svolgimento delle funzioni amministrative legate alla gestione di root (questa funzione, tuttavia, non comprende l'autorizzazione alle modifiche, integrazioni o cancellazioni di file di zona *root* e la diffusione

[12] Così L. Abba, *Internet governance: un nuovo campo di ricerca interdisciplinare riguardo a l'Internet del futuro,* 11 marzo 2009, consultabile all'indirizzo http://www.isoc.it/index.php?option=com_content&task=view&id=636&Itemid=21.

delle informazioni associate a tali attività, che invece costituiscono una delega o una nuova delega di domini di primo livello);

- l'assegnazione di risorse di numerazione Internet.

Gli Stati membri dell'Unione europea partecipano anche al Governmental Advisory Committee (GAC), il cui scopo principale è quello di consigliare l'ICANN sugli aspetti di politica pubblica.

Tutta la rete Internet funziona grazie al fatto che esistono i protocolli TCP/IP e - in senso stretto di *governance,* ma anche di governo della rete - grazie alla gestione del sistema di indirizzamento che è il solo che consente l'unicità garantita di un fenomeno globale. Gli attori principali sono i già citati ICANN, ISOC, WIPO e ITU. Questi attori ed i rappresentanti dei governi nazionali hanno la possibilità di intervenire sui criteri che consentono alla Rete di funzionare, e lo fanno attraverso la migliore collaborazione possibile. In senso largo la *governance* di Internet ha a che fare con tutti i problemi giuridici che sono affrontati localmente dagli Stati nazionali, globalmente attraverso strutture sopranazionali, o direttamente attraverso trattati internazionali. La collaborazione e la competizione vanno di pari passo ed è necessario trovare soluzioni che soddisfino gli interessi contrapposti che si contendono la nuova isola.

5. La giurisprudenza

Sul tema di cui si tratta comincia ad esserci anche giurisprudenza nazionale in certi Paesi particolarmente sviluppati, ma anche sovranazionale nei tribunali esistenti. Limiterò la mia analisi a questi ultimi – anche per ragioni di spazio – perché le pronunce di tali tribunali rappresentano, a mio avviso, una decantata visione giudiziaria del tentativo sempre presente di regolare in eccesso, al fine di limitarlo, un fenomeno che per definizione risulta difficilmente controllabile. Il *Panopticum* di Jeremy Bentham è il sogno di molti potenti della Terra, che però in Internet è difficile applicare.

Più in particolare, dunque, mi limiterò a ricordare due sentenze della Corte europea dei diritti umani, che trovo molto significative: la prima, *Dupuis and Others v. France*, n. 1914/02; la seconda, *Eerikäinen and Others v. Finland*, n. 3514/02.

Di seguito riporto alcuni estratti dai comunicati dell'Ufficio stampa della Corte che riassumono i contenuti delle pronunce richiamate.

(1)

La Cour européenne des Droits de l'Homme a communiqué aujourd'hui par écrit son arrêt de chambre dans l'affaire *Dupuis et autres c. France* (requête n· 1914/02).

La Cour conclut, à l'unanimité à la violation de l'article 10 (liberté d'expression) de la Convention européenne des Droits de l'Homme. (L'arrêt n'existe qu'en français.)

...

Article 10

La Cour relève que la condamnation des requérants constitue une ingérence dans leur droit à la liberté d'expression, que cette ingérence était prévue par le code pénal français et qu'elle avait pour but légitime de protéger le droit de G.M. à un procès équitable dans le respect de la présomption d'innocence.

...

La Cour rappelle à cet égard que la Convention ne laisse guère de place pour des restrictions à la liberté d'expression dans le domaine du discours politique ou des questions d'intérêt général et que les limites de la critique admissible sont plus larges à l'égard d'un homme politique, visé en cette qualité, que d'un simple particulier. Or, s'il n'était pas lui-même un homme politique, G.M., alors un des principaux collaborateurs du président Mitterrand, présentait toutes les caractéristiques d'un homme public influent, évidemment impliqué dans la vie politique et ce, au plus haut niveau de l'exécutif.

… la Cour rappelle qu'une atteinte à la liberté d'expression peut risquer d'avoir un effet dissuasif quant à l'exercice de cette liberté, que le caractère relativement modéré des amendes, comme c'est le cas en l'espèce, ne saurait suffire à faire disparaître.

En conclusion, la Cour estime que la condamnation des requérants s'analyse en une ingérence disproportionnée dans leur droit à la liberté d'expression et qu'elle n'était donc pas nécessaire dans une société démocratique. Elle conclut donc à la violation de l'article 10.

(2)

Eerikäinen et autres c. Finlande (requête n. 3514/02)

Les requérants sont : *Yhtyneet Kuvalehdet*, une société d'édition ; son ancien rédacteur en chef, Matti Paloaro, un ressortissant finlandais né en 1942 et aujourd'hui décédé ; et un journaliste indépendant, Pentti Eerikäinen, un autre ressortissant finlandais, né en 1946 et habitant à Kauvatsa (Finlande). Invoquant l'article 10 (liberté l'expression) de la Convention européenne des droits de l'homme, ils se plaignaient d'avoir été condamnés par la Cour suprême à verser des dommages-intérêts en raison d'un article écrit par M. Eerikäinen en 1997 au sujet d'une action pénale alors en cours dirigée contre une femme d'affaires accusée d'avoir fraudé la sécurité sociale et des compagnies d'assurances. La Cour constate que le compte rendu de l'affaire pénale dans l'article en cause était fondé sur des faits publics, portait sur une question d'intérêt général légitime et visait à contribuer au débat public. Elle conclut que, en communiquant au public l'identité de la femme d'affaires accusée, les requérants n'ont pas outrepassé les bornes et que, en condamnant ceux-ci à verser des dommages-intérêts, le gouvernement finlandais a méconnu l'article 10 de la Convention.

6. Conclusione veloce

Trattare Internet come un sistema ci ha consentito di esaminare i suoi elementi peculiari, e cioè l'ambiente, la struttura e il meccanismo. Ci ha consentito, inoltre, di studiare le sue procedure interne e di verificare che anche sotto il profilo giuridico-politico Internet si presenta come un insieme degno di speciale attenzione, perché mai studiato sistemicamente. Ed è un peccato, perché dall'ottica del sistema è più facile rilevare quali siano le caratteristiche e le pratiche che favoriscono la sua coesione ed il suo sviluppo e quali, al contrario, ne minacciano la sopravvivenza. Meglio ancora, per un'analisi giuridico-politica considerare Internet come sistema ci consente di discutere concretamente quale parte dei componenti o del rapporto con l'ambiente o della propria struttura e soprattutto del meccanismo si possa migliorare.

Il punto *dolens* è costituito dalla mancanza di una coscienza universale su questo strumento dalle potenzialità ancora non sviluppate, strumento che necessita di una regolazione adatta alle sue particolari funzioni.

Regolare è relativamente facile, soprattutto con riguardo ad una materia sconosciuta; non bisogna tuttavia dimenticare che la regolazione di Internet richiede una visione che tenga conto del carattere universale dello strumento e, soprattutto, dell'importanza di tutelare la libertà di creazione e di circolazione di dati, idee, conoscenze.

Sulla *governance* molto si sta facendo, e direi con ottimi risultati: dall'eliminazione del pericolo della limitatezza degli indirizzi IP, passando dal PV4 al PV6, fino alla discussione di una *Bill of Rights* per Internet.

Poco invece, si sta facendo in materia di governo vero e proprio. Ad essere sinceri, infatti, manca ancora uno *status* giuridico internazionale forte di Internet. Uno *status* che riconosca la sua universalità e quindi renda più difficili gli interventi intempestivi degli Stati nazionali contrari allo sviluppo, all'utilità e, in una parola, alla libertà di/in Internet.

Alcuni Stati, come Brasile ed Argentina, hanno chiesto che l'ICANN passi sotto la guida dell'Onu per liberarsi dello storico controllo del Ministero del commercio estero nordamericano. A mio avviso, si tratta di una misura pericolosa, perché l'Onu ha un'organizzazione "troppo deliberativa" mentre a capo di Internet occorre un organismo che decida con molta efficienza e tempestività; basti pensare al fatto che la velocità delle innovazioni degli utenti supera di gran lunga la capacità di previsione degli esperti.

Personalmente vedo di buon occhio la sparizione della tutela nordamericana, ma ciò deve accadere senza traumi per il "meccanismo", e dunque il primo requisito è e deve essere la continuità e l'efficienza di Internet.

E poi, supposto che si risolva il caso dell'ICANN, occorrerebbe intervenire anche sulla disciplina di tutti gli altri enti che regolano la vita di Internet: ISOC, WIPO e ITU. Senza nulla togliere alla frase precedente, credo sia arrivata l'ora di prendere il toro per le corna e di auspicare quindi, anche in seno all'Onu, la creazione di un comitato o di una agenzia indipendente sul modello dell'ISO o dell'Agenzia per la sicurezza nucleare: un ente cioè che regoli tutto il governo di Internet, dalle norme tecniche ai vincoli giuridici, concepiti come detto nei paragrafi precedenti. Un ente, in definitiva, che si dedichi alla formulazione di regole sovranazionali destinate a limitare l'arbitrarietà degli Stati nazionali.

I presupposti di fatto ci sono tutti; le conoscenze scientifiche, giuridiche ed amministrative pure. Occorre allora un colpo d'ala di natura politica, ma presto.

Sarebbe bello e significativo se la Rivista che oggi ci ospita, che ha segnato un periodo importante nello studio del rapporto tra l'informatica e il diritto, potesse accogliere le proposte concrete destinate alla creazione della ridetta "Agenzia unica del governo di Internet". Sarebbe questo, infatti, il maggior contributo alla sua *governance.*

Haud tamen audaci Turno fiducia cessit[13]

[13] Virgilio, *Eneide,* Libro X, Verso 284.

L'Internet *Governance* in Italia

ALESSANDRO NICOTRA*

1. INTRODUZIONE

Definire o circoscrivere cosa si debba intendere per Internet *Governance* non è cosa semplice, sia per una questione meramente terminologica, sia per la complessità di questa nuova materia di studio che richiede, in virtù della sua rilevanza intersettoriale e delle nuove tecnologie in continua evoluzione che la sottendono, un approccio multidisciplinare e dinamico.

Le espressioni "gestione di Internet" o "governo della Rete", usate per tradurre Internet *Governance* in italiano, sono formalmente corrette, ma nella sostanza risultano essere fuorvianti e limitative in quanto richiamano alla mente un modello di amministrazione e di definizione delle regole "dall'alto", da parte di un potere e di un'amministrazione centrali. Esattamente il contrario, quindi, di quanto avvenuto con lo sviluppo e la diffusione di Internet, le cui regole si sono determinate sulla base del *rough consensus and running code* ed il cui controllo centrale è sempre stato mantenuto al minimo livello indispensabile giusto per garantire l'unitarietà degli indirizzamenti, tramite l'allocazione degli indirizzi numerici (IP) ed alfanumerici (*Domain Names*).

Sebbene sia nata da finanziamenti del Dipartimento della Difesa degli Stati Uniti, Internet, in quanto rete di reti, si è sviluppata in modo decisamente libertario e destrutturato. La questione del "governo della Rete", agli albori, era limitata quasi esclusivamente alla risoluzione di problemi di natura tecnica e pratici: si trattava, in sostanza, di scegliere e gestire i

* L'Autore è avvocato, consigliere di ISOC Italia ed esperto di Internet *Governance*. Collabora con la Cattedra di Informatica giuridica della Facoltà di Giurisprudenza dell'Università degli Studi di Milano, come cultore della materia, e con il Ministero della Giustizia, come formatore, nell'ambito del "processo civile telematico".

protocolli in grado di far funzionare una rete informatica ovvero di connettere e di far dialogare tra loro gli utenti di diversi computer. La stessa affermazione del protocollo base di Internet, il TCP/IP, a scapito del protocollo ISO/OSI, concepito negli anni '80 dalle principali case costruttrici di elaboratori per poter assicurare la loro interoperabilità in rete, si ebbe per motivi squisitamente tecnico-funzionali: il TCP/IP era più semplice, il suo sviluppo grazie ai summenzionati finanziamenti americani era in uno stadio più avanzato rispetto al protocollo ISO/OSI ed era divenuto già lo standard di interconnessione usato per comunicare tra gruppi di ricercatori statunitensi ed europei[1].

A partire dal 1998, il governo degli Stati Uniti, con la pubblicazione del libro bianco pubblicato da Clinton e Gore, iniziava di fatto il processo di privatizzazione, a livello globale, per la gestione di Internet e, a tal fine veniva creato un ente privato: l'ICANN[2] (*Internet Corporation for Assigned Names and Numbers*) che si facesse carico della gestione tecnica della Rete. Gli U.S.A., attraverso il proprio *Department of Commerce*, avrebbero dovuto mantenere la loro supervisione su ICANN sino al completamento di questo processo di delega e di trasferimento. Nel mentre, complice la diffusione dei computer ed una vertiginosa crescita esponenziale dei dispositivi connessi (si andava già delineando la cosiddetta "società dell'informazione"), Internet è divenuta una "infrastruttura critica" a livello transnazionale e mondiale, che ha contribuito, in modo del tutto peculiare, al fenomeno della cd. "globalizzazione"[3] o "mondializzazione"[4].

Risulta più agevole, ripercorrendo la giovane storia della Rete, comprendere il perché si sia passati da un significato stretto dell'Internet *Governance*, intesa come gestione tecnica di Internet (afferente cioè alla gestione del DNS, dei *Root Server*, delle infrastrutture e degli standard tecnici), ad un'ac-

[1] S. TRUMPY, *Commenti a rfc3271*, in http://rfc3271.org/comments/trumpy_07-09-2003.html.

[2] Emblematico ed esemplificativo è il documento *Internet Domain Name System Structure and Delegation* (*ccTLD Administration and Delegation*) consultabile all'indirizzo http://www.icann.org/en/icp/icp-1.htm.

[3] Intesa come unificazione dei mercati e interconnessione delle singole economie.

[4] Si tratta di quel fenomeno per cui alcuni problemi politici, economici e sociali acquisiscono una dimensione e una portata di risonanza mondiale.

cezione più estesa nella quale rientrano tutta una serie di altri aspetti correlati, quali ad esempio: la neutralità della Rete, il diritto ed i costi di accesso, il rispetto delle libertà fondamentali sulla gestione dei contenuti, la tutela della proprietà intellettuale, le politiche fiscali, la sicurezza, l'individuazione di ciò che è reato e la correlata punibilità o repressione e via discorrendo.

In seguito al percorso tracciatosi con il *World Summit on Information Society* (WSIS), che ha individuato le più salienti problematiche della società dell'Informazione, si è tentato a livello internazionale di dare alla Internet *Governance* una definizione operativa, idonea ad abbracciare tutti i possibili aspetti connessi o ricollegabili all'utilizzo della Rete e si è addivenuti formalmente ad una proposizione di principio secondo la quale "la Governance di Internet è lo sviluppo e l'applicazione da parte dei governi, del settore privato e della società civile, nei loro rispettivi ruoli, di principî, norme, regole, procedure decisionali e programmi condivisi che determinano l'evoluzione e l'uso di Internet".

2. Dal WSIS all'IGF

Le Nazioni Unite e l'*International Telecommunication Union* (ITU), mediante l'organizzazione di due Summit (*World Summit on Information Society*) che si sono svolti a Ginevra nell'autunno 2003 ed a Tunisi nell'autunno del 2005, hanno messo a fuoco ed affrontato il problema di fondo, ossia come trattare in modo globale le infrastrutture dell'informazione e come elaborare delle *public policies* condivise.

Il coinvolgimento dei privati e della cd. società civile è risultata, sin da subito, ineluttabile ed ineludibile sia per la struttura (aperta e basata su protocolli di pubblico dominio) che per la natura (universale e decentrata alla stesso tempo) di Internet. Inoltre, il meccanismo di condivisione e selezione funzionale che ne ha da sempre contraddistinto la gestione tecnica, ha suggerito il tentativo di adoperare per la gestione "politica" della Rete lo stesso metodo del *rough consensus* che, attraverso l'elaborazione delle *Request for Comments* (RFC), ne aveva determinato il successo.

2.1. Il WSIS di Ginevra

Nel WSIS del 2003 vengono proclamati l'impegno ed il desiderio, da parte delle delegazioni dei governi partecipanti, di costruire una società

dell'informazione inclusiva ed incentrata sulla persona, orientata allo sviluppo e nella quale ognuno possa creare, accedere, utilizzare e condividere informazioni e conoscenza, per realizzarsi e migliorare la propria qualità di vita. Viene, inoltre, redatto un *Piano di azione* e si prende atto che Internet è un elemento centrale dell'infrastruttura dell'emergente società dell'informazione, pur riconoscendo che esistono punti di vista diversi sull'adeguatezza delle istituzioni esistenti e dei meccanismi previsti per la gestione dei processi e dello sviluppo di politiche relative alla Rete.

Viene anche acclarato che le questioni di Internet *Governance a* livello internazionale devono essere necessariamente trattate in maniera coordinata e, per tale motivo, è stato chiesto al Segretario generale delle Nazioni Unite di creare un *Working Group on Internet Governance* (WGIG). Tale gruppo ha così consentito una piena ed attiva partecipazione al processo in corso dei governi, del settore privato e della società civile, sia da parte dei paesi avanzati che da parte di quelli in via di sviluppo, mediante il coinvolgimento di organizzazioni intergovernative, internazionali e di gruppi interessati a preparare il terreno delle negoziazioni per la seconda fase del WSIS, da tenersi a Tunisi nel novembre 2005.

Da ultimo, il WGIG ha stabilito che al centro del dibattito del secondo summit dovevano essere trattate, tra gli atri, i seguenti aspetti:

a) l'elaborazione di opportuni documenti finali, con l'intento di consolidare il processo di costruzione di una società dell'informazione globale e di ridurre il divario digitale;

b) la modalità per dar seguito ed implementare il Piano di azione di Ginevra, su scala nazionale, regionale ed internazionale, facendo appello alla partecipazione di tutti i relativi *stakeholder,* coordinando i risultati a livello di Nazioni Unite.

In verità, il WGIG arriva, nel suo rapporto finale, ad ipotizzare diversi scenari e a formulare alcuni modelli operativi basati vuoi su una modifica sostanziale di ICANN, vuoi sulla trasformazione od evoluzione del Governmental Advisory Committee (GAC), che aveva affiancato ICANN sin dalla sua creazione, al fine di favorirne la legittimazione e l'auspicata collaborazione privato-pubblico per la gestione internazionale e futura di Internet. Ma, come è facile intuire, l'adozione condivisa a livello universale di regole sostanzialmente "politiche" risulta essere un traguardo ben più difficile da raggiungere rispetto alla creazione e

all'efficacia, funzionale e verificabile empiricamente, di protocolli meramente tecnici.

2.2. Il WSIS di Tunisi

La "Dichiarazione dei principî" e il "Piano di azione" di Ginevra, se, da una parte, contribuiscono in modo essenziale a definire il quadro della cd. società dell'informazione, dall'altra, lasciano aperta ed irrisolta la questione relativa alla *Governance* della Rete.

Nonostante le diverse posizioni politiche assunte da alcuni governi e nonostante la oggettiva impossibilità di pervenire ad una codificazione di regole universalmente accettate ed adottate, il summit di Tunisi è riuscito a produrre due risultati concreti:

- la definizione della così detta *enhanced cooperation*, che prefigura il compimento della internazionalizzazione e della privatizzazione della gestione del sistema di indirizzi della rete Internet (*Domain Name System*);

- un piano quinquennale per lo IGF (*Internet Governance Forum*), cui è stata delegata la discussione dei temi della *Governance*, tanto in senso stretto che nella sua accezione più estesa, ovvero sia con riguardo agli aspetti legati alla gestione dell'infrastruttura della Rete sia rispetto a quelli legati ai contenuti.

In particolare, con l'articolo 29 della Agenda di Tunisi, venivano sanciti i principi generali sulle necessarie modalità di gestione di Internet, e cioè attraverso un processo multilaterale, multi-*stakeholder*, trasparente e democratico.

2.3. L'Internet Governance Forum

I ruoli e le responsabilità degli *stakeholder*, suddivisi in tre categorie – governi, settore privato e società civile –, erano stati già definiti dal "Rapporto del WGIG" del luglio 2005, ma è solo con la creazione dell'*Internet Governance Forum* internazionale, dopo il WSIS di Tunisi, che si individua una concreta modalità di partecipazione aperta, libera e trasparente, oltre che di interconnessione, anche politica, tra tutti i soggetti potenzialmente interessati. Il *Forum* dovrebbe rappresentare l'occasione e lo strumento funzionale per allargare le discussioni sulle tematiche più salienti e scottanti della Rete a tutti i potenziali gruppi d'interesse, compresi i singoli individui.

L'IGF di per sé è un organismo privo di poteri decisionali che mira a facilitare il dialogo sullo sviluppo del sistema Internet, favorendo altresì la creazione di cosiddette "coalizioni dinamiche", ossia di gruppi di lavoro aperti ed informali che si attivano per affrontare singole questioni od specifici argomenti e per sottoporre le proposte così maturate nelle sedi decisionali più opportune. L'eventuale adozione di tali proposte, comunque, non può che avvenire su base volontaria, come peraltro avviene per gli standard di Internet. L'IGF, quindi, non ha il potere di sostituire o modificare attuali accordi, meccanismi, ma può eventualmente emanare raccomandazioni elaborate con il contributo degli utenti della rete. Il suo scopo principale non è quello di svolgere una funzione di controllo o di sostituirsi a qualsivoglia istituzione o organizzazione esistente, ma piuttosto quello di riuscire a coinvolgere gli *stakeholder* esistenti, interconnetterli e trarre vantaggio dalle loro competenze.

Già durante il primo IGF internazionale, svoltosi con successo nel novembre 2006 ad Atene, emergeva chiaramente l'importanza di replicare ed estendere questo processo di contribuzione, di condivisione e di partecipazione alle singole LIC (*Local Internet Community*), creando al loro interno degli *Internet Governance Forum* aventi carattere omogeneo o nazionale.

3. La Rete in Italia

L'Italia è stata fra i primi Paesi a raccogliere l'appello e l'opportunità di costituire un *Internet Governance Forum* nazionale, ma più in generale è stata uno dei Paesi più apprezzati e più attivi sul fronte della promozione e della diffusione, ad ogni livello, della "cultura della Rete".

Del resto, lo sviluppo di Internet in Italia ha una storia che è utile ripercorrere, anche solo per sommi capi ed in modo estremamente sintetico, se si vuole capire il modo in cui si è arrivati dal primo collegamento alla costituzione dell'IGF Italia.

3.1. Dal CNR-CNUCE al CNR-IIT

Le radici di Internet in Italia risalgono ai primi anni '70 e si intrecciano fondamentalmente col trasferimento di *know how* dalla ricerca sulle reti (e dalle reti della ricerca) alla interconnessione di computer. Nel 1973 il CNUCE (Centro Nazionale Universitario di Calcolo Elettronico di Pisa) viene incorporato nel CNR (Consiglio Nazionale delle Ricerche) e nel

1976 mette a punto il servizio di RPCNET, ovvero quella che sarebbe diventata la prima rete a commutazione di pacchetto dati fra diversi elaboratori, e che venne utilizzata presso il CNR dal 1979 al 1985. Lo studio su come far interagire diversi elaboratori, infatti, era divenuta una questione fondamentale per la realizzazione di infrastrutture di comunicazione in grado di scambiarsi i dati scientifici elaborati da fisici e ricercatori.

Il CNR-CNUCE ha svolto un'attività pionieristica in questo campo, seguendo sia lo sviluppo dei protocolli di comunicazione ISO/OSI che di quelli TCP/IP. Attraverso il canale satellitare SATnet nell'aprile del 1986 veniva realizzato il primo collegamento permanente italiano con la rete ARPAnet[5] – progenitrice di Internet – ovvero con il team di scienziati e tecnici che, a partire dalle Università del Sud California, costituirà il fulcro dello IANA (*Internet Assigned Numbers Authority*), organismo che aveva allora la responsabilità dell'assegnazione degli indirizzi IP.

Con la pubblicazione della RFC1591[6], relativa alla gestione del DNS, si inizia a generare una vera e propria infrastruttura globale di comunicazione: veniva infatti introdotto un meccanismo di delegazione della "porzione di quegli spazi nominativi denominati *top level domains*" (la maggior parte dei quali costituiti da due lettere indicanti il rispettivo codice secondo il noto standard di codifica ISO3166)[7].

La funzione di allocare gli indirizzi della rete, per quanto riguarda l'Italia, veniva affidata nel 1987 dallo IANA proprio al CNR-CNUCE. Nel 1988 il "Reparto applicazioni telematiche" del CNUCE, integrato di competenze sistemistiche e di risorse per far fronte alle esigenze dell'utenza (l'arrivo delle tecnologie web), si trasforma nell'Istituto di Applicazioni Telematiche (IAT del CNR), che inizia a gestire il *Name Server* autoritativo per il *Top Level Domain* ".it", creando al tempo stesso l'embrione di ciò che oggi è il *Registro .it*. Infine, nel 2002, le conoscenze,

[5] A.B. BONITO, ET AL., *Brevi norme operative per la gestione del butterfly internet gateway*, Internal note CNR-CNUCE-B4-88-036, 1988 (http://puma.isti.cnr.it).

[6] J. POSTEL, *Domain Name System Structure and Delegation*, rfc1591, http://www.ietf.org/rfc/rfc1591.txt?number=1591.

[7] L'ISO3166 è uno standard per la codifica geografica dei nomi degli Stati il cui nome ufficiale è *Codes for the Representation of Names of Countries and Their Subdivisions* (Codici per la rappresentazione dei nomi dei paesi e delle loro suddivisioni).

le competenze e la delega per la gestione del *Registro .it*, sono passate all'Istituto di Informatica e Telematica del CNR (IIT).

Il CNR-IIT è un istituto di ricerca, valorizzazione, trasferimento tecnologico e formazione a livello nazionale e internazionale nel settore delle tecnologie dell'informazione e della comunicazione e nel settore delle scienze computazionali che ha al suo interno consolidate competenze in settori di ricerca e sviluppo (quali "Internet delle cose" e "Internet dei servizi"), che spaziano dalle reti telematiche ad alta velocità, alla sicurezza e *privacy*, alle tecnologie innovative per il *web*, e che includono anche nuove tematiche relative alla *Governance* dell'Internet del futuro.

Lo stesso CNR - attraverso il CNUCE, prima, lo IAT, a seguire, e lo IIT, poi - è stato fondatore e promotore della Internet SOCiety (ISOC)[8] l'organizzazione internazionale di supporto e coordinamento della Rete Internet. L'ISOC è impegnata ad assicurare il libero sviluppo, l'evoluzione e l'utilizzo di Internet a beneficio di tutti i suoi utenti. Essa ha quindi un ruolo determinante nella definizione, nella revisione e nella messa a punto della *Governance* per Internet.

3.2. Dalle Reti di ricerca all'Internet commerciale

Analogamente a quanto avvenuto negli Stati Uniti, anche in Italia, quindi, lo sviluppo e l'uso della Rete sono stati all'inizio appannaggio esclusivo degli ambienti accademici e di ricerca. La comunità degli utenti di Internet, sino al 1992, era per lo più composta da fisici, da matematici e, più in generale, da ricercatori scientifici.

A partire dal 1992 le richieste di registrazione dei domini iniziano a crescere ed il CNUCE, grazie anche alla collaborazione con il GARR[9], organizza il servizio *Network Information Service* per la gestione del *nameserver* Internet-DNS del dominio top-level .it e per la gestione del Registro dei domini italiani. In questa fase si riscontrano ancora problemi prevalentemente di natura tecnica e tecnologica. Con l'offerta di connessione

[8] Vedi http://www.isoc.it.

[9] Il GARR (Gruppo per l'Armonizzazione delle Reti della Ricerca) è l'ente italiano (oggi strutturato in consorzio) che si occupa di gestione ed ampliamento della rete telematica nazionale ad altissima velocità delle università e della ricerca interconnessa con tutte le reti della ricerca europee e mondiali.

alla Rete anche da parte di soggetti privati (gli *Internet Service Provider*) la comunità Internet italiana iniziava ad allargarsi richiedendo una riorganizzazione del servizio di registrazione. Nel 1996 il CNR garantiva la funzione di *Registration Authority* del dominio .it mediante utilizzo di risorse proprie, ma iniziava a coinvolgere anche gli ISP commerciali nel processo di *Governance* in senso tecnico della rete italiana. Un esempio di tale coinvolgimento può essere rinvenuto nella nascita del gruppo aperto di discussione ITA-PE, che riuniva gli esperti italiani, i primi *provider/maintainer* e gli appassionati di Internet, attraverso il contributo dei quali venivano predisposte le primissime regole per l'assegnazione ed il funzionamento di Internet in Italia.

Un primo tentativo istituzionale per costituire in Italia un dialogo multi-*stakeholder* si ebbe nel 2005 con l'organizzazione di un Tavolo di consultazione sulle tematiche che sarebbero state discusse nel *World Summit on the Information Society* (WSIS), tavolo fortemente voluto dall'allora Ministro per l'innovazione, on. Lucio Stanca. L'esperienza risultò estremamente innovativa e molto importante per allargare la partecipazione ed il coinvolgimento attivo di tutti i soggetti coinvolti nella gestione della Rete.

Questo processo di confronto e coinvolgimento tra i diversi soggetti interessati, grazie alle sollecitazioni ed agli sforzi compiuti in particolar modo dal CNR e da ISOC Italia, è proseguito, in modo insolitamente *bipartisan*, anche durante le due legislature immediatamente successive: prima con il Ministro per le riforme e l'innovazione nella pubblicazione amministrazione, prof. Luigi Nicolais, che istituiva un Comitato consultivo per la predisposizione delle linee di azione italiane per contribuire all'*Internet Governance Forum internazionale*, e poi con il Ministro per la pubblica amministrazione e l'innovazione, prof. Renato Brunetta.

4. L'IGF Italia

Nel maggio del 2008 a Roma si teneva il primo incontro preliminare dell'*Internet Governance Forum* Italia, tenuto a battesimo a Cagliari nell'ottobre dello stesso anno. In quella sede vennero affrontate le tematiche centrali discusse durante l'*Internet Governance Forum* internazionale, e cioè: *Critical Internet Resources; Access; Diversity; Security; Openness; Emerging Issues*. Fu l'occasione, tra l'altro, di condividere le esperienze di governo locale

di Internet, di analizzare il rapporto tra politica ed Internet e di introdurre la proposta di una Carta dei diritti di Internet. Nell'ottobre del 2009 il secondo IGF Italia venne organizzato a Pisa dal già citato Istituto di informatica e telematica del CNR, divenendo una delle più importanti occasioni d'incontro dell'intera comunità Internet italiana. In tal modo l'IGF Italia ha risposto di fatto all'invito del Parlamento europeo a promuovere iniziative nazionali analoghe agli appuntamenti tenutisi a livello globale. Di notevole importanza, in parallelo con l'IGF internazionale previsto a Vilnius in Lituania nel prossimo settembre 2010, dovrebbe, infatti, risultare l'IGF Italia organizzato a Roma per la fine di novembre dello stesso anno[10].

La fase "politica" o, meglio ancora, la fase costituente per la *Governance* di Internet appare ad oggi ancora ad uno stadio iniziale e dal futuro incerto.

Alcuni elementi certi possono, tuttavia, essere individuati: "la rete funziona per distribuzione e fondamentalmente sottrazione di poteri: funziona per competenze riconosciute (tipicamente ai pionieri della prima e vigente generazione, ripetiamo); funziona per metodo sperimentale (un protocollo "passa o non passa" alla versione standard nel corso di un processo di laboratorio); funziona per *rough consensus* (che la comunità, semplicemente, convalida o meno, e molto praticamente, nel riscontro quotidiano di modelli concorrenti da parte di milioni di utilizzatori)"[11].

In definitiva, dunque, senza la partecipazione e senza la definizione di regole condivise tra gli *stakeholder* Internet semplicemente non funziona e si spegne.

[10] Vedi http://www.igf-italia.it.

[11] L. ABBA, G. GIUNCHI, *Futuro della gestione internazionale di Internet*, in "Quaderni dell'Internet italiano", collana Internet Governance, 2005.

La qualificazione giuridica del nome a dominio

RITA ROSSI*

1. PREMESSA

Il dibattito sulla natura del nome a dominio, le sue peculiarità tecniche e il conflitto con preesistenti diritti di terzi ha preso vigore intorno alla metà degli anni novanta con la diffusione dell'Internet commerciale[1]. L'intuizione delle capacità insite nel nuovo mezzo di comunicazione, indispensabile ad operare nel mercato globale, ha spinto soggetti privati e imprese a richiedere nomi a dominio richiamanti segni distintivi, nomi di persona, testate giornalistiche, aventi un particolare attraente contenuto, già in titolarità di altri soggetti.

Agli inizi degli anni 2000, per il diffondersi di fenomeni di accaparramento e conseguente speculazione commerciale, la questione si pone all'attenzione della stampa, dei giuristi, della politica[2]. Allo scopo di mettere ordine in materia furono presentati disegni di legge, non tradottisi

* L'Autrice è primo tecnologo presso l'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche (IIT-CNR); responsabile dell'Unità Aspetti legali e contrattuali del Registro .it e docente al Master in Tecnologie Internet organizzato dal Dipartimento di Ingegneria dell'informazione dell'Università di Pisa in collaborazione con lo IIT del CNR.

[1] Si vedano in proposito gli articoli pubblicati su interlex, www.interlex.it dove, già intorno alla metà degli anni novanta, possono rinvenirsi interessanti contributi riguardanti il conflitto fra segni distintivi e nomi a dominio. Si veda in particolare A. MONTI, 8.09.97, *Prime indicazioni sulla natura giuridica del nome a dominio*, in cui l'Autore commenta l'ordinanza del 2 agosto 1997 resa a seguito di un ricorso *ex* art. 700 c.p.c. dal Tribunale di Roma, o quella del 10 luglio 1997 emanata dal Tribunale di Milano per il dominio portaportese.it, su http://www.interlex.it/nomiadom/a_monti9.htm.

[2] Per quanto riguarda il nostro Paese il problema si pose con forza a seguito dell'apertura che si ebbe nel registro italiano il 15 dicembre del 1999 con cui furono ammessi alla registrazione i soggetti comunitari e fu tolto il limite di un solo dominio per ogni impresa. Si

poi in norme organiche, volti a definire competenze, natura e norme di funzionamento del settore[3].

Nelle idee di chi riteneva i nomi a dominio una risorsa tecnica alla quale, in caso di contrasto con un segno distintivo, ben potevano adeguarsi le normative dell'ordinamento e di chi invece invocava, in virtù della profonda diversa natura del nuovo segno, modifiche legislative *ad hoc*, la soluzione adottata col decreto legislativo 10 febbraio 2005 n. 30, recante il codice della proprietà industriale, lascia spazio ancora a dubbi e perplessità, posto che il testo legislativo si occupa solo dei nomi a dominio aziendali e non definisce l'ambito di applicazione del nuovo bene enucleato, completamente avulso dal concetto della territorialità, proprio dei tradizionali segni[4].

2. La qualificazione tecnica del nome a dominio

Sotto il profilo tecnico e funzionale "il nome a dominio è un codice mnemonico che facilita l'accesso ad una o più risorse di rete, di per sé caratterizzate da un indirizzo numerico, secondo quanto specificato dai protocolli IPS". Lo standard IPS, Internet Protocol Suite, costituisce l'insieme dei protocolli su cui funziona Internet. Ciò è quanto si può agevolmente constatare dalla lettura del Regolamento di assegnazione e gestione dei nomi a dominio del Registro italiano[5] che ne valorizza la funzione tecnica,

ricorda che l'allora direttore dello IIT, presso cui opera il Registro italiano, Prof. Franco Denoth, ricevette una lettera dalla Presidenza del Consiglio con la quale si chiedeva, nell'attesa di un intervento organico, di limitare la registrazione di nomi e cognomi ai casi in cui fosse provato il titolo all'uso del richiedente. In altri Paesi la questione è sorta antecedentemente, l' "Anticybersquatting act" statunitense è infatti del novembre 1999.

[3] Si veda il disegno di legge "Passigli" sui nomi a dominio. Il disegno Passigli recante "Disciplina dell'utilizzazione dei nomi per l'identificazione di domini Internet e servizi di rete"era stato assegnato alla Commissione giustizia del Senato il 23 maggio 2000. Esso stabiliva sanzioni severe allo scopo di scoraggiare gli abusi sui nomi a dominio e prevedeva la creazione di un'Anagrafe dei domini comprendente solo quelli registrati conformemente al disegno stesso e con la previsione di cancellare le altre registrazioni non conformi.

[4] Si confronti A. Sirotti Gaudenzi, *Codice della proprietà industriale,* Rimini, Maggioli, 2005, in cui l'autore, nel fare una ricognizione degli istituti oggetto del nuovo Codice, sottolinea il perdurare di problematiche attinenti il nome a dominio.

[5] Cfr. *Regolamento di assegnazione e gestione dei nomi a dominio nel ccTLD.it*, vers. 6.0 del 19 giugno 2009; 1.2.1. Nomi a dominio, in http://www.nic.it/documenti/regolamenti-e-linee-guida/regolamento-assegnazione-versione-6.0.pdf.

di identificatore di rete[6]. Un nome a dominio consente all'utente di individuare un computer presente sulla rete Internet, senza necessità di conoscere l'indirizzo IP[7], utilizzandone la traduzione letterale, più facile da ricordare, attraverso una serie di funzioni automatizzate[8]. Il nome a dominio non conosce alcun confine ed ogni nome a dominio in qualsiasi TLD è ugualmente accessibile da qualsiasi luogo purché vi sia un accesso ad Internet.

La disciplina in materia di nomi a dominio costituisce un servizio della società dell'informazione e a questo riguardo qualsiasi Paese comunitario voglia regolamentare questa particolare risorsa tecnica è tenuto a comunicarlo alla Commissione europea[9]. Il Regolamento (CE) n. 733/2002 del Parlamento europeo e del Consiglio del 22 aprile 2002 relativo alla messa in opera del dominio di primo livello .eu, al considerando n. 3, ne riporta una precisa definizione funzionale "3) I domini di primo livello costituiscono parte integrante dell'infrastruttura di Internet e svolgono un ruolo di primo piano ai fini dell'interoperabilità del World Wide Web ("WWW" o "Web") su scala mondiale. Grazie al collegamento e alla presenza consentiti dall'assegnazione dei nomi di dominio e dei relativi indirizzi, gli utilizzatori sono in grado di rintracciare gli elaboratori e i siti web sulla rete. I domini di primo livello costituiscono inoltre parte integrante di ogni indirizzo Internet di posta elettronica".

[6] Si legga lo scritto del 1996 di S. LE GOUEFF, P. MENCHETTI nel contributo *Convergence between Telecommunications and Audiovisual: Consequences for the Rules Governing the Information Market – IPR and Treatment of Media*, European Commission dove si esprimeva chiaramente che "domain name is a way to find a server on a network which delivers digital information in association with naming code, which is issued by the organization responsible for the administration of the network in the country where the server is located". Cfr. http://ec.europa.eu/archives/ISPO/legal/en/converge/960430/960430.html.

[7] In pratica se cambiasse il gestore presso cui è ospitato il sito web associato all'indirizzo di rete www.nic.it (per esempio passando dalla rete della ricerca GARR a Telecom Italia o a Infostrada), gli indirizzi IP dove è raggiungibile il sito varierebbero, dato che ogni gestore di servizi di rete Internet ha degli indirizzi a lui assegnati; tuttavia l'utente, digitando sul suo browser www.nic.it potrebbe comunque accedere al sito web che gli interessa, senza nemmeno sapere che l'indirizzo IP è cambiato.

[8] A. SIROTTI GAUDENZI, *Internet e diritto: problemi e soluzioni,* Bologna, Gedit, 2001.

[9] Commissione delle Comunità Europee, doc. COM(2003) 69 definitivo, "Relazione della Commissione al Parlamento Europeo e al Consiglio – valutazione dell'applicazione della Direttiva 98/34/CE nel settore dei servizi della società dell'informazione".

3. L'Autorità italiana di registrazione. Il Registro.it

Presso l'Istituto di Informatica e Telematica del CNR[10] è stabilito Il Registro del ccTLD "it", cui compete la registrazione e gestione dei nomi a dominio nell'ambito del *country code Top Level Domain* "it". Il predetto affidamento all'Istituto di Informatica e Telematica, già Istituto CNUCE, è concesso a fronte di una delega IANA - Internet Assigned Numbers Authority[11] oggi proveniente dalla Internet Corporation for Assigned Names and Numbers (nel seguito ICANN)[12]. Al riguardo si deve sottolineare che nell'ottobre del 2007 il rapporto fra ICANN e l'Istituto è stato formalizzato in uno specifico accordo scritto.

Nessuna norma nazionale definisce ufficialmente le funzioni di Registro di ccTLD. Peraltro, l'art. 2 a) del Regolamento comunitario 733/2002/CE istitutivo del ccTLD "eu" fornisce una definizione ufficiale che si attaglia perfettamente a qualsiasi Registro di ccTLD all'interno dell'Unione europea. Su tale base il Registro del ccTLD "it" può essere definito come l'organismo al quale sono affidate l'organizzazione, l'amministrazione e la gestione del dominio di primo livello "it", tra cui la manutenzione delle corrispondenti banche dati e dei servizi correlati di interrogazione destinati al pubblico, la registrazione dei nomi a dominio, la gestione del Registro dei nomi a dominio, la gestione dei *server* dei nomi a dominio di primo livello del Registro e la diffusione dei *file* di zona relativi ai domini di primo livello.

[10] Lo IIT ha lo scopo di svolgere ricerca tecnologica nel settore delle applicazioni telematiche e delle reti di comunicazione e progettare servizi innovativi curandone la sperimentazione.

[11] Le deleghe erano annunciate pubblicamente sul sito di IANA, dove sono ancora reperibili all'indirizzo: http://www.iana.org/cctld/cctld.htm. Sulla natura di IANA/ICANN vedi *infra* par. 3.

[12] Gli organismi internazionali menzionati operanti nel governo di Internet hanno curato sin dagli albori problemi tecnici e strategici riguardanti lo sviluppo della rete, fornendo alla comunità internazionale pareri ed indirizzi sulle politiche e sui problemi gestionali della rete, fino ad arrivare alla creazione di un sistema procedurale di assegnazione e gestione dei nomi a dominio omogeneo. Quest'ultimo costituisce uno strumento indispensabile per consentire l'identificazione univoca di ogni utente collegato con Internet. Su tale organismo possono leggersi i diversi articoli di Sergio Baccaglini apparsi su Interlex.it nel periodo giugno-luglio 2001, tra cui *ICANN, poca storia, molti problemi*, in http://www.interlex.it/nomiadom /indice.htm.

4. Gli organismi internazionali che operano nella rete e le normative tecniche di riferimento

Il sistema di assegnazione dei nomi a dominio è governato a livello mondiale dagli organismi statunitensi che operano per lo sviluppo della rete. L'IANA, oggi ICANN ha, fra gli altri, il compito di provvedere alla delega dei gTLD (*general Top Level Domain*) e dei ccTLD (*country code Top Level Domain*) ai vari organismi di registrazione[13]. ICANN è un ente statunitense senza scopo di lucro che opera su delega del Dipartimento del Commercio USA. Le sue attività ed i suoi atti sono riconosciuti nel nostro ordinamento nazionale in conformità del Trattato di amicizia, commercio e navigazione fra la Repubblica italiana e gli Stati Uniti d'America del 2 febbraio 1948, reso esecutivo con legge 18 giugno 1949, n. 365.

La rete dispone di un cospicuo *corpus* di norme tecniche e standard operativi emessi dagli organismi che operano nel mondo Internet, che prendono abitualmente il nome di RFC (http://www.ietf.org/rfc.html), equiparabili a tutti gli effetti alle norme tecniche emesse dall'ISO nel settore dell'informatica o dall'ITU per il settore della telefonia fissa e mobile. L'Istituto di Informatica e Telematica del CNR, Registro.it attua le norme tecniche volontarie nel settore di Internet adottate dalla Internet Engeenering Task Force (IETF) e in parte trasposte a livello nazionale in specifiche norme tecniche, quali il Regolamento di assegnazione dei nomi a dominio nel ccTLD .it, già Regole di *naming* e procedure tecniche di riassegnazione[14]. Ai fini dell'applicazione della direttiva 98/34/CE, come

[13] A. Ambrosiani, A. Monti, *Trademark Online domini internet: procedure e leggi*, Milano, Hops libri, 2001, per una disamina fra i TLD generici e i geografici anche relativamente alle regole e alle operazioni nell'ambito dei gTLD e ccTLD.

[14] IANA nel 1994 ha emesso lo RFC 1591, reperibile all'indirizzo ftp://ftp.nic.it/rfc/rfc1591.txt, che fissa i criteri generali di funzionamento dei registri ccTLD, lasciando a questi totale autonomia organizzativa. ICANN nel 1999 ha emesso un ulteriore documento ICP1, reperibile all'indirizzo http://www.icann.org/icp/icp-1.htm, che precisa alcuni concetti espressi nel RFC 1591, senza aggiungere precisazioni per quanto riguarda l'organizzazione dei registri. Ulteriori documenti emessi da ICANN sono: ICP-2 e ICP-3 concernenti il Registrante, il contatto amministrativo e tecnico necessari a garantire l'operatività del nome a dominio. Altri documenti da parte di fonti autorevoli si sono occupati dei criteri di gestione dei ccTLD; questi sono: il "Principles for Delegation and Administration of country code Top Level Domains", o Principî per la gestione e la

modificata dalla direttiva 98/48/CE, recepita in Italia a mezzo del d.lgs. 23 novembre 2000 n. 427 ed ulteriori modifiche ed integrazioni, per ciò che concerne le regole tecniche relative ai servizi della società dell'informazione la Commissione Europea ritiene che: "I nomi di dominio vanno considerati una categoria speciale, ma di particolare importanza, perché non esiste attualmente una normativa europea in materia. È dunque auspicabile che gli Stati membri abbiano un minimo di coerenza nella gestione dei loro nomi di dominio per evitare la frammentazione del mercato interno." Da parte sua, come citato sopra, la Comunità ha sviluppato un nome di dominio europeo ".eu" sulla base dei regolamenti CE 733/2002 e CE 784/2004.

5. Il regolamento per l'assegnazione e gestione dei nomi a dominio nel ccTLD .it

Il Regolamento di assegnazione e gestione dei nomi a dominio nel ccTLD.it[15], sulla base del quale il Registro opera, ha subito, in quest'ultimo decennio, continui aggiornamenti ed evoluzioni, sia sotto il profilo

delega dei ccTLD (http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm), emesso dal Governmental Advisory Committee di ICANN ed il "Best practice for the ccTLD managers", o migliori pratiche per i gestori dei ccTLD" (http://www.centr.org/docs/legal/best-practice.html), emesso da CENTR (Council of European National Top Level Domain Registries). Il primo affronta in particolare il rapporto raccomandato tra i governi, i registri nazionali e ICANN esprimendo il concetto che il registro gestisce un bene pubblico e che quindi deve agire nell'interesse della Local Internet Community (di seguito LIC), con una qualche forma di riconoscimento da parte del governo. Il secondo afferma principî non discordanti con quanto precede e dà dei criteri per assicurare un buon funzionamento delle attività principali del registro.

[15] Già definito "Regole di Naming e Procedure Tecniche di Registrazione". La definizione delle procedure tecniche e regole di Naming è stata assolta, fino al 31 dicembre 2003, dalla Naming Authority italiana (NA). In proposito va ricordato che prima del 31 dicembre 2003 il Registro .it era strutturato in due organismi: la Naming Authority italiana (NA) con funzioni normative e la Registration Authority italiana (RA) con funzioni gestionali e operative. Oggi entrambe le funzioni sono confluite nel Registro del ccTLD .it, presso lo IIT del CNR. L'attività di normazione è svolta dal Registro, con l'ausilio dalla Commissione per le regole e procedure tecniche del Registro del ccTLD.it (c.d. Commissione Regole), organo di natura consultiva. Cfr. fra gli altri E. Fogliani, *Recenti sviluppi nell'Internet Governance italiana: la nuova "Commissione per le regole" del registro del ccTLD .it*, in "Rivista di diritto dell'informazione e dell'informatica", 2004, n. 6, pp. 791 e ss.

della procedura strettamente tecnica, che di quella regolamentare. Sensibili le modifiche con riguardo alla modalità di registrazione[16], al trattamento dei dati[17], all'accesso ai documenti e alle informazioni, alla risoluzione delle dispute, alla modulistica, all'accreditamento degli enti cui è affidata la risoluzione extragiudiziale delle dispute[18].

Con decorrenza dal 19 luglio 2009, a seguito dell'implementazione del nuovo sistema sincrono di registrazione, sono entrati in vigore i nuovi Regolamenti e precisamente: Regolamento di assegnazione e gestione dei nomi a dominio nel ccTLD .it[19]; Regolamento per la risoluzione delle dispute nel ccTLD.it[20]; Linee guida per la gestione delle operazioni sui nomi a dominio nel ccTLD.it nel sistema sincrono[21]; Linee guida per la gestione delle operazioni sui nomi a dominio nel ccTLD.it nel sistema asincrono[22]; Linee guida per la risoluzione delle dispute nel ccTLD .it[23].

[16] Fino all'entrata in vigore del nuovo regolamento di assegnazione la registrazione del nome a dominio poteva realizzarsi solo mediante l'invio cartaceo al Registro del documento chiamato "Lettera di Assunzione di Responsabilità" - LAR che contiene oltre ai dati del richiedente una serie di dichiarazioni e attestazioni, fra cui quella di non ledere diritti di terzi, etc. Oggi queste dichiarazioni e attestazioni sono contenute nel "Documento di registrazione" con cui l'utente può, tramite accordo telematico, richiedere la registrazione del nome a dominio. Cfr. Regolamento di assegnazione e linee guida, cit.

[17] Il tema del corretto trattamento dei dati nel settore dei nomi a dominio è di estrema importanza ed è stato oggetto di parere anche da parte del Gruppo articolo 29 (direttiva 45/96/CE), nonché di osservazioni nell'ambito degli organismi internazionali che si occupano della rete quali ICANN, CENTR, l'Autorità Garante per il trattamento dei dati personali. Si veda nella Newsletter 18-24 giugno 2001 del Garante per la protezione dei dati personali il seguente contributo: *Nomi di dominio su Internet: problemi di privacy* (da un articolo di Brian Krebs su Newsbytes dell'11 giugno). A tale questione, per l'economia di questo lavoro, non può farsi cenno neppure in via di estrema sintesi.

[18] Per un ampio excursus sulla risoluzione stragiudiziale dei conflitti per i domini .com, .net, .org,.it, con specifico riferimento alla prima fase implementativa di queste procedure, si veda L. TURINI, *Domini Internet e risoluzione dei conflitti*, in "Il Sole 24 ore", Milano, 2000.

[19] Http://www.nic.it/documenti/regolamenti-e-linee-guida/regolamento-assegnazione-versione-6.0.pdf.

[20] Http://www.nic.it/documenti/regolamenti-e-linee-guida/risoluzione-delle-dispute-nel-cctld.it-regolamento-versione-2.0-ultimo-1.

[21] Http://www.nic.it/documenti/regolamenti-e-linee-guida/Linee_guida_sincrono_ver-1.2.pdf.

[22] Http://www.nic.it/documenti/regolamenti-e-linee-guida/Linee-guida-asincrono.pdf.

[23] Http://www.nic.it/documenti/regolamenti-e-linee-guida/linee-guida-legali.pdf.

La procedura sincrona permette la registrazione di un nome a dominio in tempo reale attraverso degli intermediari tecnici, definiti Registrar[24], i quali possono operare solo previo accreditamento da parte del Registro; tali imprese sono autorizzate a iscrivere il nome a dominio direttamente nel data base dei nomi a dominio assegnati (DBNA), senza l'intervento manuale dell'operatore del Registro, come è stato fino a tempi recentissimi. Certamente questo potrà aprire ulteriori problematiche dato che viene meno il controllo a priori che il predetto organismo svolgeva durante l'operazione manuale di inserimento della Lettera di Assunzione di Responsabilità (LAR) col quale l'utente chiedeva la registrazione del nome a dominio.

Il Regolamento ribadisce alcuni principî noti fra cui l'assegnazione dei nomi a dominio sulla base dell'ordine cronologico di arrivo della richiesta, il ripudio dell'accaparramento sistematico[25] o *cybersquatting*, la regola secondo cui un nome a dominio può essere assegnato al registrante soltanto dopo che il richiedente abbia indicato i propri dati, accettato le condizioni e le responsabilità stabilite per la registrazione di un nome a dominio nel ccTLD.it,; il rispetto delle norme in materia di trattamento dei dati; la responsabilità del registrante riguardo alla registrazione del nome a dominio stesso, nonché delle informazioni e dei servizi eventualmente attivati sullo stesso. Il nome a dominio peraltro può essere revocato o sospeso per ordine dell'autorità giudiziaria o nell'ipotesi in cui all'esito dei previsti controlli da parte del Registro la registrazione non risulti regolarmente effettuata. Un nome a dominio può inoltre essere ceduto a seguito di accordo fra le parti o per successione *mortis causa*.

È prevista la possibilità per il terzo di ricorrere alla procedura alternativa di risoluzione delle dispute, al fine di ottenere la riassegnazione del

[24] Il Registrar è un fornitore di servizi accreditato che ha un contratto con il Registro in base al quale può registrare e gestire i domini .it in modalità sincrona, principalmente per conto di terzi. Si veda il contratto fra il Registro e i Registrar alla url http://www.nic.it/documenti/contratti/contratto-registrar.pdf#sincrona.

[25] Come noto il fenomeno del *cybersquatting* e del *domain grabbing* ricorre quando viene registrato un nome di dominio corrispondente ad un nome o ad un marchio altrui, di solito rinomato, per scopi meramente speculativi, ad es. con l'intento di cedere la registrazione a titolo oneroso al legittimo titolare del marchio. Cfr. L. TURINI, *op. cit.*

nome a domino[26], previo svolgimento della procedura di opposizione presso lo IIT; ciò in presenza di determinati presupposti che il ricorrente è tenuto a provare [27]. Il compito di dirimere questo genere di conflitti è affidato a studi professionali o società comunitarie accreditate dal Registro[28]. Nelle sue linee essenziali il sistema ricalca l'impostazione data da ICANN alla risoluzione dei conflitti nei gTLD, general Top Level Domain, e negli altri registri, i ccTLD, che abbiano voluto aderirvi[29].

È importante sottolineare che i nomi a dominio sono assegnati in uso ai registranti. Tale espressione ha talora sollevato osservazioni anche per la contraddittorietà fra l'attribuzione della qualifica di assegnatario e la possibilità di trasferire tale risorsa a terzi.

I Regolamenti sopra indicati rappresentano sostanzialmente una normativa di carattere pattizio che ha origine nell'autonomia lasciata al

[26] La procedura alternativa di risoluzione dei conflitti sui nomi a dominio è entrata in vigore nel Registro italiano il 28 luglio 2000 sulla base della procedura implementata da ICANN il 24 ottobre del 1999. Cfr. L. TURINI, *op. cit.*

[27] Art. 3.6. Procedura di riassegnazione di nome a dominio sottoposto a procedura di opposizione, principi generali. **"**Sono sottoposti alla Procedura i nomi a dominio per i quali un terzo (denominato "ricorrente") affermi che: a) il nome a dominio contestato sia identico o tale da indurre confusione rispetto ad un marchio su cui egli vanta diritti, o al proprio nome e cognome; e che b) l'attuale assegnatario (denominato "resistente") non abbia alcun diritto o titolo in relazione al nome a dominio contestato; ed infine che c) il nome a dominio sia stato registrato e venga usato in mala fede. Se il ricorrente prova che sussistono assieme le condizioni "a)" e "c)" di cui sopra ed il resistente non prova a sua volta di avere diritto o titolo in relazione al nome a dominio contestato, quest'ultimo viene trasferito al ricorrente". Cfr. http://www.nic.it/documenti/regolamenti-e-linee-guida/risoluzione-delle-dispute-nel-cctld.it-regolamento-versione-2.0-ultimo-1.

[28] Cfr. il documento "Modalità di accreditamento dei Prestatori del Servizio di risoluzione delle dispute nell'ambito del ccTLD.it"; http://www.nic.it/documenti/Modalita-accreditamento-psrd.pdf. Il ricorso ai PSRD permette all'utenza, sulla base di costi e tempi contenuti, di chiedere la sola riassegnazione del nome a dominio. Al 30 giugno 2010 nel ccTLD .it si contano 464 procedure di cui in 309 casi l'esperto ha trasferito il nome al ricorrente, in 64 casi la richiesta è stata respinta e in 79 casi la procedura si è estinta.

[29] Cfr. la Uniform Dispute Resolution Policy di ICANN disponibile alla url http://www.icann.org/en/udrp/udrp-policy-24oct99.htm. Vi sono alcune differenze fra le UDRP di ICANN e, ad esempio le procedure di riassegnazione italiane, visto che in queste ultime, a differenze di quanto avviene con ICANN, si può chiedere solo la riassegnazione e non la cancellazione del nome a dominio. Per una ricerca degli organismi ai quali può essere affidata la risoluzione delle dispute. Cfr. http://www.icann.org/en/dndr/udrp/approved-providers.htm.

Registro di dotarsi di un'adeguata regolamentazione e non sono costituiti da specifiche norme nazionali di diritto positivo.

6. La giurisprudenza in materia di nomi a dominio

Ripercorrere un'analisi dei molti contributi giurisprudenziali di quest'ultimo decennio non sembra consono all'economia di questo lavoro[30]. L'orientamento giurisprudenziale e di dottrina, largamente prevalente, poi recepito nel Codice della proprietà industriale[31], anche in materia cautelare[32] ha ricondotto il nome a dominio nei confini della tutela dei segni distintivi. Si è sostenuto chiaramente che il nome a dominio costituisce "un nuovo segno distintivo dell'impresa, suscettibile, in quanto tale, di entrare in conflitto con altri segni distintivi, in base al principio dell'unità dei segni distintivi desumibile dall'art. 13 legge marchi" (Tribunale di Napoli, 26 febbraio 2002). È stato evidenziato come il nome a dominio dovesse essere equiparato all'insegna poiché il sito può essere considerato il luogo virtuale dove l'imprenditore contatta il cliente al fine di condurre a termine con esso il contratto. (Trib. di Milano, 10 giugno 1997). Si è riconosciuta la possibilità di rivendicare, nei confronti di un sito Internet, la protezione offerta dalla legge per i titoli delle testate giornalistiche e per le riviste, in considerazione di quanto riportato all'articolo 100 della legge sul diritto d'autore, che vieta di riprodurre tali titoli in altre opere della stessa specie o carattere, se non siano decorsi due anni da quando è cessata la pubblicazione del giornale[33]. Nel rapporto col nome di una persona merita segnalare la nota sentenza del Tribunale di Torino del 2004 in cui il giudice ha riconosciuto il diritto al nome della persona

[30] La produzione della dottrina e della giurisprudenza è ormai molto consistente e ad essa si rimanda. Si citano, fra gli altri, C. Galli, *I domain names nella giurisprudenza*, Milano, Giuffrè, 2001. L. Turini, *op. cit.*, A. Sirotti Gaudenzi, *Codice della Proprietà industriale*, cit., P. Sammarco, *Il regime giuridico dei nomi a dominio*, Milano, Giuffrè, 2002; la rivista on-line Interlex che da anni pubblica contributi in questa materia (http://www.interlex.it/testi/na020226.htm.

[31] Vedi *infra* par. 6.

[32] Vedi Tribunale di Roma, ordinanza del 2 agosto 1997; Tribunale di Firenze, 16 dicembre 2004.

[33] Vedi la sentenza riferita al nome a dominio "Foroit", Tribunale di Modena, 23 ottobre 1996; e al nome a dominio "portaportese.it", Tribunale di Roma, 2 agosto 1997.

famosa statuendo il principio per il quale il titolare di un nome notorio ha il diritto di lucrarvi[34].

7. L'ordinamento giuridico italiano in materia di nomi a dominio

7.1. La natura del nome a dominio nel codice delle comunicazioni elettroniche

L'intervento del legislatore italiano in materia di nomi a dominio si è realizzato mediante provvedimenti giuridici aventi scopi profondamente diversi: da un lato, la necessità di regolamentazione del settore delle comunicazioni elettroniche e, dall'altro, la ridefinizione e accorpamento dei diritti in materia di proprietà industriale.

Il Codice delle comunicazioni elettroniche introdotto col d.lgs. 1° agosto 2003, n. 259, prevede all'art. 15 "Numerazione, assegnazione dei nomi a dominio e indirizzamento" un ruolo di vigilanza da parte del Ministero delle attività economiche statuendo l'impegno dello stesso, per il tramite dell'Istituto Superiore delle comunicazioni e delle tecnologie dell'Informazione (ISCOM), al controllo dell'assegnazione di tutte le risorse nazionali di numerazione e la gestione del piano nazionale di numerazione, garantendo che a tutti i servizi di comunicazione elettronica accessibili al pubblico siano assegnati numeri e blocchi di numeri adeguati, compresi nomi a dominio e loro indirizzamento[35].

Il Codice citato interviene per recepire la direttiva comunitaria 2002/19/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime (direttiva accesso), la direttiva 2002/20/CE, del Parlamento europeo e del Consiglio, del 7 marzo 2002,

[34] In Italia, come anche in Germania, il diritto al nome può essere utilizzato anche da persone giuridiche come diritto da tutelare in relazione all'uso da parte di terzi di un nome a dominio corrispondente o che induce in confusione rispetto alla denominazione della loro organizzazione o ente. Negli Stati Uniti non esiste invece una protezione generale del diritto al nome.

[35] Art. 15, co. 1: "(…) Il Ministero [delle attività economiche], altresì, vigila sull'assegnazione dei nomi a dominio e indirizzamento.". Ai sensi del D.P.R. 28 novembre 2008, n. 197, la funzione di vigilanza è attribuita all'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM). Articolo 15, co. 6: "Il Ministero e l'Autorità [AGCOM], al fine di assicurare l'interoperabilità completa e globale dei servizi, operano in coordinamento con le organizzazioni internazionali che assumono decisioni in tema di numerazione, assegnazione di nomi a dominio e indirizzamento delle reti e dei servizi di comunicazione elettronica".

relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica (direttiva autorizzazioni); la direttiva 2002/21/CE, del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro), la direttiva 2002/22/CE, del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (direttiva servizio universale)[36]. Dall'insieme della normativa comunitaria sopra citata scaturisce indubbiamente una funzione tecnica del nome a dominio già inquadrato come risorsa di numerazione e di assegnazione nell'ambito della più generale regolamentazione dei servizi di comunicazione elettronica. Il nome a dominio è da concedersi in uso ai richiedenti nel rispetto dei principî di equità e pari accessibilità al servizio. Principî sui quali l'attuale ISCOM (già Ministero delle Comunicazioni) è chiamato a svolgere attività di vigilanza.

Per completezza, appare opportuno ricordare che l'ultimo paragrafo del considerando n. 20 della direttiva 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (c.d. direttiva quadro) recita come segue: "Le disposizioni della presente direttiva non definiscono nuovi settori di competenza per le autorità nazionali di regolamentazione nel settore dell'assegnazione dei nomi di dominio e dell'indirizzamento in Internet".

7.1. La natura del nome a dominio nel codice sulla proprietà industriale

Il Codice della proprietà industriale (d.lgs. 10 febbraio 2005, n. 30)[37] dà un nuovo assetto alla materia dei diritti di proprietà industriale, prima disciplinati in normative sparse. L'art. 2 del predetto Codice distingue in

[36] Per una compiuta disamina delle normative circa l'afferenza del nome a dominio al settore della numerazione nelle telecomunicazioni, nonché del pacchetto di direttive comunitarie di liberalizzazione ed armonizzazione in materia di telecomunicazioni conosciuto come "1998 regulatory package", anche antecedentemente all'entrata in vigore del d.lgs. 259/03, si veda: P. MENCHETTI, *I nomi a dominio e la tutela dei segni distintivi in Internet*, articolo pubblicato a margine del convegno del 19 ottobre 2001 presso la Camera di Commercio di Lecco.

[37] Emanato in attuazione della legge delega 12 dicembre 2002, n. 273 recante "Misure per favorire l'iniziativa privata e lo sviluppo della concorrenza" (G.U. 14 dicembre 2002, n. 293, suppl. ord. n. 230).

primo luogo fra diritti "titolati" derivanti dalla brevettazione e dalla registrazione, quali le invenzioni, i modelli di utilità, le nuove varietà vegetali, i marchi, i disegni e modelli, le topografie dei prodotti a semiconduttori e diritti "non titolati", ovvero i segni distintivi diversi dal marchio registrato, le informazioni aziendali riservate, le indicazioni geografiche e le denominazioni di origine[38].

I nomi a dominio aziendali, ossia quella risorsa utilizzata dall'imprenditore con funzione di segno distintivo secondo i contenuti e le finalità di cui all'art. 2555 c.c.[39], rientrano dunque fra i diritti non titolati[40]. Sul punto l'art. 22 (Unitarietà dei segni distintivi)[41] ha stigmatizzato la prassi

[38] Art. 2 (Costituzione ed acquisto dei diritti): "1. I diritti di proprietà industriale si acquistano mediante brevettazione, mediante registrazione o negli altri modi previsti dal presente codice. La brevettazione e la registrazione danno luogo ai titoli di proprietà industriale.

2. Sono oggetto di brevettazione le invenzioni, i modelli di utilità, le nuove varietà vegetali.

3. Sono oggetto di registrazione i marchi, i disegni e modelli, le topografie dei prodotti a semiconduttori.

4. Sono protetti, ricorrendone i presupposti di legge, i segni distintivi diversi dal marchio registrato, le informazioni aziendali riservate, le indicazioni geografiche e le denominazioni di origine.

5. L'attività amministrativa di brevettazione e di registrazione ha natura di accertamento costitutivo e dà luogo a titoli soggetti ad un regime speciale di nullità e decadenza sulla base delle norme contenute nel presente codice".

[39] A. SIROTTI GAUDENZI, *Codice della Proprietà Industriale*, cit.; G. FLORIDIA, *Il riassetto della proprietà industriale*, Milano, Giuffrè, 2006.

[40] Va evidenziato che sulla bozza del codice furono espresse osservazioni da parte di Confindustria; tra queste la difficoltà di irrigidire una funzione tecnica in stretti principi di carattere giuridico che mal si sarebbero adattati a una realtà mutevole come quella di Internet; l'esistenza di regole di registrazione efficaci ad opera dell'Autorità italiana di registrazione; ed ancora, la mancanza di un raccordo con l'art. 15 del Codice delle comunicazioni. Cfr. A. SIROTTI GAUDENZI, *Codice della Proprietà Industriale*, cit.

[41] L'art. 22 (Unitarietà dei segni distintivi) prevede il divieto di "adottare come ditta, denominazione o ragione sociale, insegna e nome a dominio aziendale un segno uguale o simile all'altrui marchio se, a causa dell'identità o dell'affinità tra l'attività d'impresa dei titolari di quei segni ed i prodotti o servizi per i quali il marchio è stato adottato, possa determinarsi un rischio di confusione per il pubblico che può consistere anche in un rischio di associazione fra i due segni". Il divieto "si estende all'adozione come ditta, denominazione o ragione sociale, insegna e nome a dominio aziendale di un segno uguale o simile a un marchio registrato per prodotti o servizi anche non affini, che goda nello Stato di rinomanza se l'uso del segno senza giusto motivo consente di trarre indebitamente vantaggio dal carattere distintivo o dalla rinomanza del marchio o reca pregiudizio agli stessi".

giurisprudenziale formatasi in questi ultimi anni in tema di proprietà industriale e di unitarietà dei segni distintivi disponendo il divieto dell'adozione di un segno come ditta, denominazione o ragione sociale, insegna e nome a dominio aziendale uguale o simile all'altrui marchio se, a causa dell'identità o dell'affinità tra l'attività d'impresa dei titolari di quei segni ed i prodotti o servizi per i quali il marchio è stato adottato, possa determinarsi un rischio di confusione per il pubblico che può consistere anche in un rischio di associazione fra i due segni. Se il marchio gode di rinomanza il divieto si estende anche a prodotti o servizi anche non affini, "…se l'uso del segno senza giusto motivo consente di trarre indebitamente vantaggio dal carattere distintivo o dalla rinomanza del marchio o reca pregiudizio agli stessi". Tale Codice contiene dunque un espresso riconoscimento giuridico che consacra il nome a dominio come bene economico. Tuttavia il testo normativo non ne rende una definizione sostanziale, non spiegando quali siano gli elementi che lo caratterizzano riguardo i limiti di uso, territoriali, di spazio e di specie, peculiarità imprescindibili dei tradizionali segni. Si costringe l'interprete ad operare continue distinzioni fra ciò che costituisce un bene aziendale e quindi protetto e ciò che invece non rientra nella norma del Codice. Anche sul piano soggettivo la definizione di nome a dominio aziendale presenta una certa approssimazione con riferimento ad esempio al professionista che operi su Internet per quanto questi svolga indubbiamente un'attività di carattere economico; altrettanto dicasi per l'ente pubblico che realizzi un'attività economica. Va precisato per completezza che l'art. 118, rubricato "Rivendica", dispone che un nome a dominio concesso in violazione dell'art. 22, o richiesto in mala fede, possa essere revocato al registrante da parte dell'autorità di registrazione [42]. Si è discusso, all'indomani dell'entrata in vigore del Codice, se l'autorità di registrazione fosse titolare di un potere proprio di revoca, indipendentemente da un'ordinanza o sentenza che si esprimesse sulla domanda giudiziale o invece se dovesse aspettarne l'esito prima di procedere. La tesi alla quale il Registro italiano si è atte-

[42] Art. 118, Rivendica "Salva l'applicazione di ogni altra tutela, la registrazione di nome a dominio aziendale concessa in violazione dell'articolo 22 o richiesta in mala fede, può essere, su domanda dell'avente diritto, revocata oppure a lui trasferita da parte dell'autorità di registrazione".

nuto è stata quella di attendere l'ordine del giudice al fine di ogni eventuale azione in merito. In ordine poi alla tutela cautelare, l'art. 133, dello stesso Codice, sancisce la possibilità che l'utilizzo del nome a dominio registrato in violazione dei diritti altrui sia inibito all'assegnatario e che si possa provvedere anche al trasferimento provvisorio al richiedente[43].

Ci si è interrogati, anche in anni antecedenti all'emanazione di questa normativa, sulla pignorabilità del nome a dominio. Per taluna dottrina non sono stati ravvisati elementi che ne impediscano l'attivazione dato che "i beni immateriali per i quali vi sia un espresso divieto sancito dalla legge o per i quali vi sia un impedimento giuridico dovuto al fatto che essi riflettono diritti personalissimi dell'individuo non possono formare oggetto di espropriazione; se, invece, essi presentano indici di commerciabilità, in quanto aventi un valore economico, possono costituire oggetto di espropriazione forzata"[44]. Si ritiene perciò che il nome a dominio in quanto bene immateriale, suscettibile di valutazione economica, possa essere sottoposto al pignoramento[45]. La predetta questione è già stata affrontata dalla giurisprudenza la quale ha dichiarato che "non é pignorabile il *domain name*, cioè l'indirizzo su internet dell'impresa, atteso che esso coincide con

[43] Art. 133 (Tutela cautelare dei nomi a dominio): "l'Autorità giudiziaria può disporre, in via cautelare, oltre all'inibitoria all'uso del nome a dominio aziendale illegittimamente registrato, anche il suo trasferimento provvisorio da parte del beneficiario del provvedimento subordinandolo, se ritenuto opportuno, alla prestazione di idonea cauzione da parte del beneficiario del provvedimento".

[44] P. SAMMARCO, *Il regime giuridico dei nomi a dominio,* Milano, Giuffrè 2002. Per l'autore, che realizza una ricostruzione del nome a dominio come bene, quest'ultimo costituirebbe "un bene ideale, frutto dell'astrazione del pensiero dato appunto dal diritto sul "nome a dominio", inteso come bene giuridico a cui si riallacciano altri diritti esclusivi previsti in capo al titolare di altri beni immateriali sottostanti. In questo modo chiaramente, la struttura del diritto come bene, da intendersi come poteri, facoltà ed obblighi, è strettamente connessa alla natura dell'originario diritto che si accompagna al primo".

[45] "Vi saranno, in ogni caso, difficoltà di ordine pratico legate alla procedura esecutiva, quali la necessarietà di una valutazione economica da affidarsi ad un terzo nominato dal giudice e, forse, la scelta delle forme dell'espropriazione, ovvero se debba essere effettuata direttamente in danno del debitore o attraverso la procedura di espropriazione presso terzi. In applicazione di tali principi, è valida l'opinione che ammette la possibilità di sottoporre ad espropriazione anche un "nome a dominio", qualora esso possa essere ritenuto dal creditore un bene idoneo a rappresentare una garanzia patrimoniale offerta dal debitore", P. SAMMARCO, *op. cit.*

la denominazione sociale della stessa. Infatti il domain name non è un diritto reale né un diritto di credito, ma un segno distintivo dell'impresa assimilabile all'insegna di talché esso non può essere né venduto, né utilizzato da terzi, senza configurare una ipotesi sia di concorrenza sleale che di pubblicità ingannevole" (Tribunale di Bologna, 22 marzo 2000).

Al fine di valutare la pignorabilità di un nome a dominio in quanto titolo di proprietà industriale è necessario partire dalle previsioni del Codice della proprietà industriale e a tal fine non sembra, a un primo esame, che l'art. 137, che dispone in ordine all'esecuzione forzata e sequestro dei titoli di proprietà industriale, abbia portata innovativa rispetto ai tradizionali principî giurisprudenziali sopra enunciati. A tale riguardo lo stesso Floridia (Presidente della Commissione ministeriale che ha redatto il Codice della proprietà industriale)[46] ritiene infatti che l'art. 137 sia applicabile solo ai cosiddetti diritti titolati di cui all'art. 2 co. 2 e 3 del Codice citato. In particolare, secondo questa dottrina, le norme del codice di procedura civile in materia di pignoramento di beni mobili contemplano esclusivamente i beni materiali, e il pignoramento del diritto di proprietà industriale *ex* art. 137 non può avvenire mediante la materiale apprensione del bene[47]. Conseguentemente, sempre secondo tale autore, il pignoramento secondo la norma in questione avviene mediante la trascrizione da compiere a pena di inefficacia entro 8 giorni dalla notifica. Ai sensi dell'art. 138 del Codice di proprietà industriale, le trascrizioni riguardano solo i diritti titolati *ex* art. 2, co. 5, del Codice della proprietà industriale. La procedura di registrazione di un nome a dominio presso il Registro.it non è riconosciuta dall'art. 2 del Codice quale procedimento costitutivo di titolo di proprietà industriale, *ex* co. 5 del predetto articolo, dato che l'elenco dei co. 2 e 3 è tassativo e gli altri diritti rientrano nel co. 4 dello stesso articolo. La predetta dottrina conclude pertanto per l'inapplicabilità del pignoramento *ex* art. 137 al nome a dominio aziendale, così come peraltro alla ditta o all'insegna.

Nella specie il Registro, a seguito di una sentenza esecutiva, ha ricevuto un provvedimento del Tribunale di Parma "Atto di pignoramento

[46] G. FLORIDIA, *op. cit.*

[47] G. FLORIDIA, *op. cit.*

mobiliare di titolo di proprietà industriale" di un nome a dominio registrato a favore del soccombente dato il valore economico del medesimo nome. La società creditrice chiedeva la sottoposizione a sequestro del nome a dominio ai sensi dell'art. 137 e ss. del Codice della proprietà industriale e dell'art. 513 e ss c.p.c., nonché la notifica al Registro dell'atto in questione al fine di provvedere alla trascrizione del pignoramento o di qualsivoglia equivalente atto o procedura volta e idonea a rendere edotti i terzi dell'esistenza di un provvedimento giudiziario/pignoramento. Il Registro in tal caso ha apposto l'annotazione di valore contestato "challenged" al nome a dominio non potendo evidentemente compiere ulteriori atti dandone nel contempo comunicazione alle parti.

Nella qualificazione del nome a dominio non può sottacersi infine la circostanza che il nome a dominio è oggetto di circolazione, mediante atto di trasferimento tra vivi o per successione, come esplicitamente disciplinato nel Regolamento di assegnazione dei nomi a dominio nel ccTLD.it, e ciò indubbiamente contribuisce alla valutazione del nome a dominio come bene giuridico suscettibile perciò di un valore economico, anche molto elevato.

8. Conclusioni

Con buona ragione può dirsi dunque che il nome a dominio genericamente definito è, *in primis*, una *risorsa* per cui mezzo l'utente Internet può sfruttare le opportunità di conoscenza, di informazione, di produzione, di occupazione proprie della rete. In questa direzione il dominio può assumere la veste di bene giuridico di recente generazione, una sorta di nuovo diritto telematico, che si configura quale interesse personale a richiedere e disporre di tale bene che deve essere garantito a chiunque. La riduzione del ragionamento a questo assunto potrebbe non rendere la complessità del problema ove l'utente voglia avere risposte e garanzie sulla certezza di esclusività di preesistenti diritti riconosciutigli dall'ordinamento giuridico. In questo ambito, come abbiamo visto nel corso di questo lavoro, alcune importanti risposte sono state date dal Codice della proprietà industriale, seppure con i limiti esaminati. Fino ad oggi, come s'è detto, le autorità di registrazione, cui è delegata la gestione dei Registri generali (gTLD) e nazionali (ccTLD), hanno operato secondo regolamenti e procedure *ad hoc*, per la maggioranza dei casi di natura consensuale, e non

legislativa, facendo indubbiamente progredire il settore[48], assicurando la diffusione capillare della tecnologia, mezzi di risoluzione alternativa delle dispute e, almeno per quanto riguarda il Registro italiano, alcuni strumenti di controllo.

Certo emerge la difficoltà di riportare ad unità i principi che governano il mondo della tecnologia e quello del diritto, quasi una sorta di istituzioni separate che rispondono a proprie, diverse, regole[49].

Internet inoltre è un fenomenale strumento di ricchezza economica e la libertà di utilizzarne tutte le potenzialità è indubbiamente rivendicata da più parti.

[48] Nell'ambito del Registro italiano i nomi a dominio sono passati da 1500 alla fine del 1995 ai quasi due milioni di nomi che saranno raggiunti a metà luglio 2010. Per il dato di registrazione degli altri Registri si confrontino le url: http://www.hosterstats.com/DomainNameCounts2010.php; http://www.verisign.com/domain-name-services/domain-information-center/domain-name-resources/domain-name-report-june10.pdf; http://www.zooknic.com/Domains/counts.html.

[49] Si veda la prefazione di T. Ballarino, *Trattato breve di diritto della rete. Le regole dell'Internet*, in AA.VV., "Trattato breve di diritto della rete. Le regole di Internet, Rimini, Maggioli, 2001. In esso l'Autore rileva come Internet rappresenti una nuova "dimensione del diritto" a cui, col tempo dovranno probabilmente applicarsi delle specifiche regole che superino gli attuali limiti derivanti dalla localizzazione degli ordinamenti.

La riservatezza dei dati personali in Internet

Le prospettive del diritto all'oblio nella società dell'informazione e della comunicazione

DANIELA MESSINA*

SOMMARIO: *1. Il diritto "di dimenticare" e "di essere dimenticati" – 2. Il difficile cammino del riconoscimento del diritto all'oblio – 3. Il legislatore e la disciplina del diritto all'oblio – 4. I tre elementi cardine del diritto all'oblio: tempo, interesse sociale e soggetti legittimati ad agire*

1. IL DIRITTO "DI DIMENTICARE" E "DI ESSERE DIMENTICATI"

Con il termine diritto all'oblio si indica, ormai in modo diffuso, la tutela del particolare interesse di una persona a non subire ulteriori lesioni della propria sfera personale causate dalla reiterazione del contenuto di una notizia, in passato legittimamente pubblicata, ma ormai priva di un interesse pubblico tale da giustificarne un'ulteriore diffusione. Si fa riferimento, in particolare, al diritto di un individuo a non vedere distorta la propria immagine attuale a causa di una nuova diffusione di notizie relative a vicende o affermazioni che in passato l'hanno visto protagonista, ma che non corrispondono più a quella che è l'attuale proiezione della propria identità all'interno della società. Appare infatti evidente che, venuta meno la "pertinenza" della notizia quale elemento fondamentale del diritto di cronaca, ridiventa primario e fondamentale il diritto dell'individuo a non veder minata la naturale evoluzione della sua personalità, il suo desiderio di condurre una vita "normale" e, soprattutto, il suo diritto a non essere identificato in modo univoco con un evento del passato.

Questa aspettativa veniva in passato sostanzialmente soddisfatta dal trascorrere del tempo, in quanto l'importanza di una notizia vantava una durata limitata nel tempo ed era destinata ad essere dimenticata col macero della carta su cui essa era impressa. Oggi, invece, le moderne tecnologie pongono il problema della concreta possibilità di "essere dimenticati", dal momento che una notizia risulta molto spesso imprigionata in una

* L'Autrice è dottoranda di ricerca in "Pubblico e privato nel diritto dell'impresa" presso l'Università degli Studi di Napoli "Parthenope".

Rete non più fisica, ma virtuale. Con l'avvento delle nuove tecnologie ad essere minacciati, infatti, non sono solo i dati personali e, ancor di più, quelli sensibili, ma è la stessa "percezione collettiva del passato" in un panorama in cui, paradossalmente, per la prima volta viene messa in discussione non la possibilità di ricordare, possibilità che anzi risulta potenziata dai nuovi metodi di archiviazione di massa delle informazioni bensì, al contrario, *il diritto di dimenticare e di essere dimenticati.*

La sostanziale "immortalità dei dati" nella Rete, inoltre, comporta che questi, se non aggiornati, siano destinati a rimanere "congelati" al momento stesso in cui vengono immessi nel circuito digitale con la rilevante conseguenza che, tramite il continuo riproporsi delle notizie, l'identità di una persona rischia di non evolversi mai, cristallizzata, immobilizzata ad un unico istante della sua vita con il pericolo, talvolta, di veder perpetuata o riproposta una "sanzione sociale" che la società virtuale sembra amplificare rispetto al mondo fisico contemporaneo[1].

In quest'ottica, la problematica del diritto all'oblio nella società dell'informazione e della comunicazione, ed in particolare in Internet, assume una sensibile rilevanza e si pone come diritto di ogni utente a veder tutelata la propria identità digitale dalla circolazione di informazioni errate, inesatte o superate. Infatti, anche – e forse – in prospettiva futura, soprattutto tutelando la proiezione virtuale della propria identità, l'individuo ha la possibilità concreta di proteggere di riflesso la propria identità reale e, quindi, il proprio ruolo all'interno della società.

2. Il difficile cammino di riconoscimento del diritto all'oblio

Come è noto, il riconoscimento in Italia di nuove situazioni giuridiche soggettive come la riservatezza, l'identità personale e, non da ultimo, il diritto all'oblio, è avvenuto solo in tempi relativamente recenti, a causa probabilmente della mancanza nell'ordinamento di una loro esplicita pre-

[1] A tal proposito, A. Papa, *Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico*, Torino, Giappichelli, 2009, pp. 135 e ss., sostiene che "Nelle società contemporanee, sempre più strutturate come *Information and Communication Societies,* si moltiplicano gli strumenti mediante i quali è possibile porre in essere processi di sanzione sociale. […] I *blog*, le camere di conversazione, i *forum* si prestano "per natura" ad essere luoghi nei quali viene data pubblicità di comportamenti ritenuti contrari alle regole sociali della comunità".

visione normativa[2] e di una accentuata, almeno in passato, assenza nella società italiana di una naturale propensione al riserbo e, sovente, al rispetto dell'altrui *privacy*. Inoltre, in ambito giurisprudenziale, dove a lungo vi è stata difformità di orientamento tra giudici di merito, convinti dell'esistenza di un diritto alla riservatezza o privatezza, anche in assenza di un esplicito riferimento nell'ordinamento italiano[3], e giudice di legittimità,

[2] Tale lacuna ha spinto la dottrina e la giurisprudenza ad interrogarsi su quale fosse il concreto contenuto degli emergenti diritti della personalità e a trovare una soluzione in merito alla questione relativa al carattere chiuso ovvero aperto della clausola di garanzia dei diritti inviolabili della persona, di cui all'art. 2 della Costituzione. Senza pretesa di esaustività cfr. P. BARILE, *Istituzioni di diritto pubblico*, Padova, Cedam, 1976; C. MORTATI, *Istituzioni di diritto pubblico*, Padova, Cedam, 1967; F. BARTOLOMEI, *La dignità umana come concetto e valore costituzionale*, Torino, Giappichelli, 1987. In particolare Baldassarre parla di "forza maieutica dell'art. 2 rispetto alla tavola dei diritti contenuta nella Costituzione" (A. BALDASSARRE, *Diritti sociali*, in "Enciclopedia giuridica", Istituto della Enciclopedia italiana, Roma 1989). A favore del carattere "chiuso" della norma P. RESCIGNO, *Personalità (diritti della)*, in "Enciclopedia Giuridica", XXIII, Roma, 1990; V. ZENO-ZENCOVICH, *Personalità (diritti della)*, in "Digesto delle Discipline Privatistiche - Sez. civile", vol. XIII, 1995. Come è noto, la dottrina è comunque pervenuta al riconoscimento dell'art. 2 come clausola "generale ed aperta", strumentale alla fondamentale funzione della Costituzione di carta espressione delle esigenze di tutela evidenziate dai consociati, anche alla luce dei continui ed inarrestabili cambiamenti della società, con il conseguente ampliamento in via di principio della categoria dei diritti della personalità costituzionalmente riconosciuti. Una volta riconosciuta la fonte di legittimazione, l'analisi interpretativa del contenuto dei diritti della personalità ha portato alla convinzione che ad essere protetta dall'ordinamento giuridico sia la persona umana nel suo complesso, quale valore unitario. Si è assistito, così, ad una progressiva "costituzionalizzazione" della personalità, dalla quale è possibile muoversi per il riconoscimento e la tutela di quei diritti che da essa promanano come molteplici raggi di luce tagliati da un unico prisma rappresentante la persona. Ecco che allora, negando l'esistenza di un *numerus clausus* di diritti della personalità, anche il diritto all'oblio è entrato a pieno diritto nel mosaico di esigenze specifiche e differenziate che vengono a comporre quell'unica, ma variegata, situazione giuridica soggettiva meritevole di tutela, trovando in essa fondamento alla propria esistenza e legittimazione al proprio riconoscimento dottrinale. Cfr. C.L. CRIPPA, *Il diritto all'oblio: alla ricerca di un'autonoma definizione*, in "Giustizia Civile", 1997, nn. 7-8, pp. 1990 e ss.; M.R. MORELLI, *voce Oblio (diritto all')*, in "Enciclopedia del diritto", Aggiornamento VI, Milano, Giuffrè, 2002.

[3] In tal senso B. MARKESINIS, G. ALPA *Il diritto alla "privacy" nell'esperienza di "common law" e nell'esperienza italiana*, in "Rivista Trimestrale di diritto e procedura civile", Milano, Giuffrè, 1997, n. 2, pp. 417 e ss., dove, in riferimento al caso Caruso, riportano il principio, affermato dai giudici di merito, secondo cui: "il nostro ordinamento, pur non prevedendolo esplicitamente, riconosce l'esistenza di un diritto alla riservatezza o privatezza, il quale si concreta nel divieto di qualsiasi ingerenza estranea nella sfera della vita privata della persona, e

contrario all'esistenza di un principio generale di riserbo[4], la problematica dell'evoluzione della persona legata allo scorrere degli anni ha tardato a trovare spazi . Il fattore temporale, anzi, è stato spesso sottovalutato, adombrato dalla notorietà dei soggetti coinvolti e dalla convinzione che la stessa celebrità giustificasse intromissioni nella loro vita privata ogni qualvolta la notizia risultava di fatto idonea ad incrementarne la relativa notorietà. In tale contesto, gli unici casi in cui si è riconosciuto a personaggi noti il diritto ad invocare la tutela della propria sfera d'intimità da tali illecite invasioni hanno riguardato esclusivamente quelle situazioni in cui l'interesse pubblico si è trasformato in una vera e propria morbosa curiosità o in un pettegolezzo relativamente a vicende non legate all'attività pubblicamente svolta[5].

Ad aprire la strada verso il riconoscimento effettivo dell'impatto del fattore temporale su una notizia già divulgata è stato, alla fine degli anni ottanta, un significativo cambiamento nella giurisprudenza della Corte di

di qualsiasi indiscrezione, da parte di terzi, su quei fatti o comportamenti personali che, non pubblici per loro natura, non sono destinati alla pubblicità delle persone che essi riguardano". A sostegno di tale interpretazione vi è un'ordinanza del 1996, in cui il Tribunale di Roma ha affermato che "la pretesa sostanziale a riappropriarsi in via esclusiva delle informazioni della propria vita privata che, benché pubblicizzate, abbiano perso di attualità, […] trae fondamento direttamente dall'art. 2 della Costituzione, inteso come clausola generale, suscettibile di assicurare copertura ai valori emergenti della persona".

[4] In tal senso B. MARKESINIS, G. ALPA, *op. cit.*, che sottolineano la risposta negativa della suprema Corte in merito alla questione relativa all'esistenza di un generale diritto alla riservatezza durante il caso Caruso. In particolare la Corte ha affermato che: "nessuna disposizione di legge autorizza a ritenere che sia stato sancito, come principio generale, il rispetto assoluto all'intimità della vita privata e tantomeno come limite alla libertà dell'arte; […] il semplice desiderio di riserbo non è stato ritenuto dal legislatore un interesse tutelabile, chi non ha saputo o non ha voluto tener celati i fatti della propria vita, non può pretendere che il segreto sia mantenuto dalla discrezione altrui; la curiosità ed anche innocuo pettegolezzo, se pur costituiscono una manifestazione non elevata dell'animo, non danno luogo ad un illecito giuridico".

[5] La piena consacrazione nell'ordinamento italiano del diritto alla riservatezza è avvenuta con la sentenza n. 2129 del 1975, della Corte di Cassazione che lo ha definito come: "tutela di quelle situazioni e vicende strettamente personali e familiari, le quali, anche se verificatesi fuori dal domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che compiute sia pure con mezzi leciti, per scopi non esclusivamente speculativi, e senza offesa per l'onore, la reputazione e il decoro, non siano giustificate da interessi pubblici preminenti".

Cassazione[6], che ha sancito il principio secondo cui l'interesse della collettività ad essere informata in modo tempestivo e completo, così da poter conoscere e semmai potersi tutelare dinanzi ad un evento particolare, viene fisiologicamente a stemperare man mano che la notizia è acquisita e fatta propria dalla comunità stessa. Si è affermata, in tal modo, l'idea che una volta che il pubblico ha ricevuto un'informazione completa circa l'accaduto e non vi siano ulteriori sviluppi in merito alla vicenda, è naturale che l'interesse collettivo venga a cadere in quanto di fatto viene a cessare la "notizia stessa". Partendo da questa considerazione, la riproposizione dell'evento passato da un lato non risulta più utile alla collettività, dall'altro è dannosa per i protagonisti della vicenda, che vedono ulteriormente ed inutilmente lesa la propria immagine.

Nonostante l'intervento della Cassazione e un'evoluzione nel tempo della sensibilità collettiva circa la tematica in oggetto, la piena consacrazione del nuovo diritto, tuttavia, è avvenuta non alla fine di un completo processo di maturazione del dibattito sul ruolo del diritto all'oblio, ma essenzialmente e di riflesso su richiesta dell'Unione europea con il recepimento della direttiva 95/46/Ce riguardante il trattamento e la libera circolazione dei dati personali, seguita dalla direttiva 97/66/Ce[7], relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle telecomunicazioni. Attualmente il diritto all'oblio trova tutela nell'art. 11, co. 1, lett. *e)* del *Codice in materia di protezione dei dati personali*[8] ma, in una società domi-

[6] Cass. civile, sez. I, 15 marzo 1986, n. 1763, RAI C. Abrescia, in DeJure.

[7] La direttiva in questione ha stabilito nello specifico che: "I dati sul traffico relativi agli abbonati e agli utenti, trattati per inoltrare chiamate e memorizzati dal fornitore di una rete pubblica e/o di un servizio di telecomunicazione offerto al pubblico, devono essere cancellati o resi anonimi al termine della chiamata, fatte salve le disposizioni dei paragrafi 2, 3 e 4", laddove i paragrafi indicati riguardano quei casi in cui i dati risultano essere fondamentali per le indagini relative ai clienti e per l'accertamento di frodi. La direttiva, inoltre, viene subito a sottolineare che la conservazione e l'utilizzo dei dati "deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività".

[8] D.lgs. 30 Giugno 2003, n. 196. L'articolo in questione stabilisce che "I dati personali oggetto di trattamento sono […] conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati". Assume particolare rilievo anche l'art. 7, co. 3, lett. b), che annovera tra i diritti di cui gode l'interessato il diritto alla "cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge

nata da tecnologie che favoriscono il ricordo in maniera automatica e spesso asettica, sono ancora molteplici gli aspetti di questa particolare situazione giuridica soggettiva ad essere oggetto di critica e di discussione.

3. Il legislatore e la disciplina del diritto all'oblio

L'analisi del nuovo ruolo assunto dalla memoria collettiva nelle moderne società dell'informazione e della comunicazione necessita di un cenno comparativo finalizzato ad evidenziare quale sia l'atteggiamento adottato dalla dottrina e dalla giurisprudenza estera dinanzi alla rivendicazione di questo nuovo diritto della personalità. A tal fine, risulta utile comparare il disegno di legge attualmente in discussione nel Parlamento italiano con un'analoga proposta oggetto di valutazione in Francia, Paese ritenuto da molti "culla del diritto all'oblio"[9]. Trattasi di due disegni di legge che affrontano in modo specifico il problema della riproposizione delle notizie in Rete, anche se focalizzati su due differenti aspetti.

In particolare, la proposta italiana è diretta a garantire il diritto all'oblio in Internet a favore delle persone già sottoposte ad indagini o imputate in un processo penale. A tal fine, essa sancisce in maniera generale il principio secondo cui "decorso un lasso temporale, variabile a seconda della gravità del reato, e salvo che risulti il consenso scritto dell'interessato, non possano più essere diffusi o mantenuti immagini o dati, anche giudiziari, che consentano, direttamente o indirettamente, l'identificazione della persona già indagata o imputata, sulle pagine Internet liberamente accessibili dagli utenti oppure attraverso i motori di ricerca, esterni al sito web sorgente". A questo principio di carattere generale fa seguito un vero e proprio elenco di sentenze-tipo, cui corrisponde indicazione del tempo massimo consentito di permanenza in Rete[10]. Il carattere automatico che la proposta sembra attri-

compresi quelli di cui non e' necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati".

[9] Si fa riferimento al disegno di legge n. 2455 presentato alla Camera dei deputati il 20 maggio 2009 dal deputato Lussana e al disegno di legge n. 93 (2009-2010) depositato in Senato il 6 novembre 2009 dai senatori Détraigne e Escoffier.

[10] Art. 1 della citata proposta di legge prevede che: "salvo che risulti il consenso scritto dell'interessato, non possono essere diffusi o mantenuti immagini e dati, anche giudiziari, che consentono, direttamente o indirettamente, l'identificazione della persona già indagata o

buire alla tutela del diritto all'oblio è, tuttavia, oggetto di perplessità perché di fatto fa proprio inevitabilmente l'orientamento, anch'esso particolarmente dibattuto, di un necessario ruolo di controllo sui contenuti disponibili in Rete da parte dei *provider*[11]. Un ruolo essenzialmente tecnico, che non prevede alcuna garanzia di proporzionalità tra interessi contrapposti. Il rischio sotteso è quello di dar vita ad una limitazione *a priori* del diritto del singolo ad essere informato; una limitazione che opererebbe automaticamente senza quella necessaria valutazione qualitativa del contenuto della notizia e della relativa importanza ai fini di un equilibrato sviluppo di una società effettivamente democratica. Diverso, invece, è l'impianto del disegno di legge presentato da due senatori francesi e attualmente in discussione. Il progetto, infatti, risulta essere di più ampia ispirazione essendo destinato a garantire la tutela dei dati personali e, più in generale, della vita privata dei soggetti che utilizzano Internet[12]. Una proposta non limitata ad una sola categoria di soggetti, perché imperniata sul concetto di *Homo numericus*, libero e protettore dei propri dati personali. Essa prevede, quindi, una tutela che opera non in maniera automatica ed indiscriminata, bensì attraverso l'intervento dell'autorità giudiziaria, l'unico soggetto in grado di entrare nel merito della questione e di garantire quel giusto bilanciamento tra interessi meritevoli di tutela, che anche lo spazio virtuale richiede. A tal fine, il disegno di legge prevede un ampliamento delle possibilità di adire un'azione giudizia-

imputata nell'ambito di un processo penale, sulle pagine internet liberamente accessibili dagli utenti o attraverso i motori di ricerca esterni al sito in cui tali immagini o dati sono contenuti, quando sono trascorsi: a) tre anni dalla sentenza irrevocabile di condanna per una contravvenzione; b) cinque anni dalla sentenza irrevocabile di condanna per un delitto, se la pena inflitta è inferiore a cinque anni di reclusione; c) dieci anni dalla sentenza irrevocabile di condanna per un delitto, se la pena inflitta è superiore a cinque anni di reclusione; d) quindici anni dalla sentenza irrevocabile di condanna per un delitto, se la pena inflitta è superiore a dieci anni di reclusione; e) venticinque anni dalla sentenza irrevocabile di condanna per un delitto, se la pena inflitta è superiore a venti anni di reclusione."

[11] Per un approfondimento cfr. A. PAPA, *op. cit.*

[12] Il disegno di legge francese, inoltre, contempla anche la tutela del diritto di proprietà intellettuale, con particolare attenzione alle giovani generazioni, integrando gli articoli ad esso dedicati dalla legge n° 2009-669, nota come Hadopi (*Haute Autorité pour la Diffusion des Ouvres et la Protection des Droits sur Internet*), che prevede la disconnessione graduale degli utenti che scaricano dalla Rete *file* coperti da *copyright* ad opera di un'agenzia creata appositamente, appunto l'Hadopi.

ria per coloro che siano impossibilitati ad esercitare il proprio diritto alla cancellazione dei dati personali; una maggiore tracciabilità, al fine di evitare una dispersione degli stessi dati; un rafforzamento del ruolo e dei poteri d'azione del CNIL, la *Commission nationale de l'informatique et des libertés*.

L'analisi delle due proposte di legge evidenzia, quindi, da un lato, la maggiore maturità della questione "oblio" in Francia. Una maturità che si lega indubbiamente a quella peculiare attenzione e sensibilità che l'ordinamento francese presenta nei confronti del rispetto alla vita privata, ritenuto diritto fondamentale, riconosciuto e consacrato dall'art. 9 del *Code Civil*. Grazie ad esso, la sfera privata degli individui vede riconosciuta a proprio favore una tutela dall'ampiezza tale da delineare un vero e proprio diritto generale della personalità, cui la giurisprudenza è tenuta a sua volta a far continuo riferimento per procedere alla tutela delle istanze di protezione emergenti. Nessuna determinazione *a priori* delle fattispecie di reato, quindi, ma un unico grande diritto alla tutela della vita privata, che guida la giurisprudenza nella valutazione caso per caso dei comportamenti suscettibili di arrecare una lesione alla vita privata altrui.

Il disegno di legge italiano, al contrario, sembra non cogliere fino in fondo il problema legato al diritto all'oblio in Rete e, in particolare, alla necessità di individuare quel difficile, ma necessario, equilibrio tra questo ed il diritto di narrare gli avvenimenti che caratterizzano la vita di una società democratica, pur nel pieno rispetto delle identità individuali. Il progetto, infatti, nell'elencare i casi, astraendoli dalle fattispecie concrete, non si sofferma sugli elementi cardine che rendono tale diritto meritevole di tutela e non soffocante le altrui libertà fondamentali, quali l'interesse pubblico alla notizia, i soggetti legittimati ad agire ed il fattore temporale.

4. I tre elementi cardine del diritto all'oblio: tempo, interesse sociale e soggetti legittimati ad agire

La tutela dell'individuo dalla riproposizione di avvenimenti che in passato lo hanno visto protagonista impone inevitabilmente di analizzare il fattore temporale, tuttavia, in un'ottica non statica, bensì dinamica. Parametro di riferimento del diritto all'oblio, infatti, non è il *passato* in sé, ma, al contrario, è il *presente* frutto dell'insieme delle scelte esistenziali dell'individuo, che il complesso dei diritti della persona tende a preservare e tutelare da

indebite interferenze esterne. Non è in sé la vetustà dei fatti a legittimare l'evocazione del diritto all'oblio, ma è il potenziale danno che il vissuto di una persona può arrecare al suo presente. Quando, infatti, il passato non risulta essere fondamentale per interpretare l'attuale ruolo dell'individuo nella società, appare ragionevole chiedere che esso rimanga nell'oblio, soprattutto quando la relativa rievocazione comporti una lesione dell'attuale identità, sociale e privata, della persona. È indubbio che le esperienze vissute inevitabilmente concorrano a delineare la personalità di un individuo, ma è altrettanto innegabile che spesso sono proprio gli errori del passato a spingere una persona a mutare il modo di condurre la propria vita con la conseguenza che non vi sia necessariamente una continuità tra l'identità passata e quella presente, potendo quest'ultima rappresentare anche un'evoluzione di tipo correttivo della prima. In questo caso, il fattore temporale rileva in termini non quantitativi, ma qualitativi: il cambiamento di un individuo, infatti, non è semplicemente determinato dal numero degli anni trascorsi dalla vicenda riproposta, come intende il disegno di legge presentato alle Camere in Italia, bensì dal modo in cui questi anni sono stati spesi a favore di un'esistenza diversa. Solo attraverso questa interpretazione il diritto all'oblio esplica in maniera corretta la sua tutela, non mettendo in pericolo il diritto di cronaca costituzionalmente garantito, né l'attività di ricostruzione storica, attività fondamentale per la corretta evoluzione della società.

Da qui la necessità che al trascorrere di alcuni anni dall'avvenimento riproposto alla collettività si associ anche il mancato interesse sociale alla notizia. Al riguardo alcuni autori affermano l'esistenza di una sorta di "presunzione in base alla quale in via di principio i fatti passati non possono essere più divulgati, per non trasformare il diritto all'informazione nella pretesa di conoscere qualsiasi avvenimento della vita altrui"[13]. D'altra parte una delle tre caratteristiche fondamentali, individuate come qualificanti una notizia, è rappresentata proprio dall'interesse ad esso rivolto dalla comunità cui è destinata. In assenza di tale interesse, la descrizione di una vicenda, pur nel rispetto dei canoni di veridicità e di continenza, viene ad essere declassata a morboso interesse della vita

[13] M. MEZZANOTTE, *Il diritto all'oblio. Un contributo allo studio della privacy storica*, Napoli, ESI, 2009, p. 123.

altrui[14]. Adottando tale interpretazione, è indubbio che ogni ulteriore diffusione di una notizia del passato richiede una giustificazione che non può che ritrovarsi in un rinnovato interesse della comunità legato all'evolversi della stessa vicenda. Altre motivazioni, non solo non comportano alcun vantaggio ai fini dell'attività di cronaca, ma causano un ulteriore danno a quella tranquillità cercata e forse trovata dai protagonisti.

Un'ultima considerazione riguarda la possibilità che la vita di una persona sia così strettamente connessa a quella del contesto sociale di appartenenza da divenire parte integrante dell'attività di ricostruzione storica di quella determinata comunità, simbolo o chiave di interpretazione narrativa di un determinato periodo. In questo caso appare possibile sottolineare come l'interesse storico divenga rilevante e, alla luce della sua fondamentale funzione al servizio dell'evoluzione della società, si pone come prevalente rispetto alla tutela del riserbo dei singoli protagonisti. La veste "storica" di questi ultimi modifica la linea di demarcazione tra sfera pubblica e privata, ponendosi come ipotesi derogatoria al diritto all'oblio, dal momento che vi sono delle vicende, così fortemente caratterizzanti il soggetto o la storia raccontata, in relazione alle quali l'imposizione dell'oblio finirebbe per svuotarne il significato, impedendo alle generazioni future di capire le dinamiche sottese ai comportamenti dei soggetti agenti[15].

[14] A tal proposito, la giurisprudenza ha individuato il significato del termine interesse sociale nell'insieme delle ragioni culturali, morali, ideali o politiche che legano fortemente la vicenda alla società cui è destinata divenendone espressione.

[15] Questo è ad esempio il caso vicenda del noto tenore Caruso. A tal proposito G. Giacobbe afferma che: "la ricostruzione delle vicende di una famiglia dei bassi di Napoli dalla quale era emerso un personaggio divenuto famoso in tutto il mondo non poteva certo essere operata in modo incisivo senza il diretto riferimento a quel personaggio". G. GIACOBBE, relazione in Gabrielli E. (a cura di), "Il diritto all'oblio. Atti del Convegno di Studi del 17 maggio 1997", Napoli, ESI, 1999, p. 36. A tal proposito si è pronunciato anche il Tribunale di Roma con la sentenza del 19 gennaio 2004, G. Caradonna v. Isole nella Rete. Il caso riguarda la citazione per diffamazione del sito *web* Isole nella Rete da parte di un deputato che, tra le altre cose, "denunciava la mancanza di interesse pubblico attuale della divulgazione della notizia della sua passata militanza politica e la conseguente lesione del proprio"diritto all'oblio" a causa della descrizione sul sito di avvenimenti passati in grado di intaccare il proprio elevato profilo professionale. Come invece sottolineato dal giudice "fuori discussione appare in proposito la pretesa di trincerarsi dietro al "diritto all'oblio", di per sé inconfigurabile in presenza - come detto - di un interesse pubblico attuale della conoscenza del proprio passato politico".

In quest'ambito, coloro che evidenziano l'esistenza di un conflitto tra il diritto all'oblio e il diritto alla storia, affermando che il primo opererebbe in termini di cancellazione indiscriminata degli eventi passati, in realtà sembrano proporre un falso problema. Il diritto ad essere dimenticati, infatti, non ha pretese di tale ampiezza e soprattutto incontra limiti forti dinanzi a tutti quegli avvenimenti per i quali l'interesse pubblico non viene mai a cessare, esistendo al contrario un obbligo morale a mantenerne vivo il ricordo. Il caso emblematico è rappresentato dalla narrazione delle vicende rientranti nel novero dei crimini contro l'umanità: in questo caso i nomi dei protagonisti, dei luoghi e la descrizione anche dettagliata degli avvenimenti non possono e non devono essere lasciati alla deriva della memoria né è possibile invocare alcun tipo d'oblio perché trattasi di vicende che appartengono alla storia dell'umanità e che come tali non divengono mai private. Anzi, la loro mancata riproposizione verrebbe a porsi in contrasto proprio con il pubblico interesse, arrecando un danno incalcolabile all'evoluzione della società umana. Ecco perché, come è stato sottolineato, il diritto all'oblio può essere qualificato come "diritto di dimenticare e non come diritto di far dimenticare, mai e comunque"[16].

[16] A. SAVINI, *Diritto all'oblio e diritto alla storia,* in "Il diritto di autore", 1997, n. 3, pp. 381 e ss.

Protecting Informational Privacy in Cyberspace: Exploring Complementary Routes

JEANNE PIA MIFSUD BONNICI*

1. INTRODUCTION

Protecting informational privacy in cyberspace is difficult. The technical infrastructure makes it remarkably easy to collect and use personal information[1], while there are few incentives in favour of the respect of privacy over use of personal information for commercial purposes. The Internet and other technologies have created new opportunities for providers of service to collect personal information easily, amass large databases of personal information and capitalize on the personal information for commercial purposes. Our very presence on the Internet leaves valuable traces that internet service providers, search engines, providers of social network sites, credit card companies, web shops etc. can exploit at times with our consent or our connivance or at times surreptitiously without caring to consider our possible opposition. These providers (and users/merchants) of personal information have become a primary threat for users' privacy, at the same time that the services they offer are simultaneously growingly indispensable for many users. More than 90% of Internet users in Europe have registered anxiety over abuse of personal information online[2]. Governments too, may be a threat to user privacy in the delivery of e-government services and the centralisation of personal information.

* The Author is Associate Professor and Rosalind Franklin Fellow, University of Groningen, The Netherlands.

[1] P. SAMUELSON, *Privacy as intellectual property?* in "Stanford Law Review", Vol. 52, 2000, p. 1125.

[2] Eurobarometer Report, *Confidence in the Information Society*, May 2009, available at http://ec.europa.eu/public_opinion/flash/fl_250_en.pdf.

To date, states have sought to protect (the fundamental right[3] of) privacy by specific personal data protection legislation and by encouraging businesses to adopt privacy policies and practices to protect consumer/user privacy. These approaches have limited effects, leaving consumers often without any protection or remedies against abusive use of their personal information. While in case of government traditional safeguards provided from fundamental human rights enforcement mechanisms are also available – there is still an option to sue governments for breaches of fundamental rights as judgements of the European Court of Human Rights show – the responsibility of private companies for breaches of informational privacy is still being worked out.

This paper reflects on the role that data protection legislation (namely as implemented in European Member States following Directive 95/46/EC and other later directives) has in the protection of informational privacy online. It looks at two specific scenarios: possible remedies where personal information has been negligently lost or stolen; and possible safeguards or remedies available when two or more private information-rich businesses merge or are taken-over online. In each scenario, it explores possible approaches that can be used to complement the current systems of protection of personal information. The paper explores two potentially complementary approaches:

The first approach is embedded in current theories of public international law arguing for private sector fundamental rights responsibility. In this part of the paper the author explores the usefulness of using developments in public international law on private sector responsibility for breaches of fundamental rights – e.g. in the case of breach of property rights or environmental rights – and the shifting of liability of private sector liability to states in cases of breaches of fundamental rights – e.g. where the state takes responsibility for breaches (of e.g. environmental protection) carried out by private companies established in its territory.

The second approach is a market-based approach using competition policy mechanisms to protect informational privacy. Traditionally, privacy law and competition law have been considered to be two separate and

[3] Protected by Article 8 of the European Convention of Human Rights.

independent areas of law with very little (if at all) in common. Recent developments[4] in the United States and Europe suggest that perhaps there is more in common between these two areas of law than first thought. This paper will describe and explain these developments.

2. Informational Privacy

Before examining the legal protection offered or that can potentially be offered to consumers to protect their personal information, it is important to define what is meant by the phrase 'informational privacy' in this paper. Three aspects of informational privacy, loosely based on Roessler's list in 'New Ways of Thinking about Privacy'[5], will be considered here.

The first element, based on the US concept of 'right to be left alone', finds that "information about a person is worthy of protection even when it involves something that occurs in public"[6]. In a European context, this element of informational privacy is often protected in press laws. The European Court of Human Rights has also had the opportunity to elaborate on the remits of this aspect of informational privacy in amongst other Von Hannover v. Germany[7]. It has considered that the absence of a remedy in relation to the publication of information relating to private affairs may constitute a lack of respect for private life. In Von Hannover v. Germany the Court acknowledged that, despite being very well known, there was no doubt that the publication by various magazines of photographs of the applicant in her daily life fell within the scope of her private life and warranted protection[8].

The second element of 'informational privacy' relates to autonomy – the ability to control what personal information is made public and what

[4] In particular following the Google-DoubleClick merger in 2007.

[5] B. Roessler, *New Ways of Thinking about Privacy*, In Dryzek J.S., Bonnie Honig J.S, Phillips A. (eds.), "The Oxford Handbook of Political Theory", Oxford, Oxford University Press, 2008.

[6] Ibid., p. 704.

[7] Von Hannover v. Germany - 59320/00 [2004] ECHR 294 (24 June 2004).

[8] D.J. harris, M. O'boyle, et al., *Harris, O'Boyle and Warbick: Law of the European Convention on Human Rights*, Oxford, Oxford University Press, p. 368.

personal information is kept private. This aspect – *informational self-determination* – is to some extent protected (in Europe) by data protection legislation.

The third element of 'informational privacy' relates to situations of abuse following from the mass collection and processing of personal information. This third aspect can cover both misuse of personal information by the state and by the private sector. It is this third aspect of informational privacy that will be given most attention in this paper.

3. Data Protection Law

Data protection legislation provides (in different ways and different extents) for the three aspects of informational privacy just described. In Europe primarily, data protection legislation is based on a fundamental right to live one's private life without unnecessary interference identified in the Universal Declaration of Human Rights and the European Convention of Human Rights (ECHR)[9]. Since the 1980s, the right to private life (envisaged in Art. 8 ECHR) has been extended to cover protection of personal information. By 1981, well ahead of the commercial introduction of the Internet, the Council of Europe had opened for signatory Convention 108 – the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – for its Member States. The main principles found in Convention 108 where later taken up by the European Union, in its Directive 95/46/EC on the protection of individuals with regard to the processing of personal data. This Directive, was agreed on in 1995 (at the start of the commercial Internet era) came into force by 1998 (at the start of the first major growth of the Internet) and is still in force today. The developments in (tele)communications technology and the use of personal data information in the offering of services are covered by another Directive – Directive 2002/58 on Privacy and Electronic Communications – introduced after the 2000, '.com' fall out.

The approach taken to the protection of personal information (in Europe) can be described as a 'fundamental rights approach' where what

[9] Article 8 - European Convention Human Rights; Article 12 – Universal Declaration of Human Rights.

is protected is not the information itself but the individual (and his/her right to a private life). Protection of personal information in data protection is based not on ownership of the personal information but on the fact that that personal information identifies the data subject. The protection attached to personal information has since 2000 been included as a separate fundamental right in the Charter of Fundamental Rights of the European Union[10].

Directive 95/46/EC establishes some fundamental principles in accordance with which personal data can be collected, processed and kept. It also gives some powers to a data subject to access, seek rectification or deletion of inaccurate or no longer appropriate information. Directive 2002/58 complements Directive 95/46/EC and applies to areas not specifically identified in Directive 95/46/EC such as treatment of traffic data, spam, cookies and confidentiality of information. This paper will not proceed with a detailed review of what these two Directives protect, instead it will focus on two scenarios of possible abuse following from the mass collection and processing of personal information where, it is argued here, the Directives do not provide enough protection.

Before proceeding with the scenarios, it is important to keep in mind that the in the US the position is somewhat different as there is no comprehensive privacy protection. Direct legislation to protect personal information has been sporadic and sectoral. Information privacy is protected only through an amalgam of narrowly targeted rules[11]. Instead the approach has been one that relies on market self-regulation, that is, protection of personal information privacy is dependent on businesses introducing self-imposed rules identifying fair information practices. To a

[10] Article 8 – Charter of Fundamental Rights of the European Union.
Article 8 - Protection of personal data 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.

[11] J. Reidenberg, *Privacy Wrongs in Search of Remedies*, in "Hastings Law Journal", Vol. 54, 2002, p. 877.

large extent, the market has had few incentives to self-regulate. In practice there are many significant gaps in protection and few clear remedies for violations of fair information practices.

4. Scenario 1: Negligent Loss or Theft of Personal Information

The first situation to be considered here is the following: The increased ease in collecting personal information (on the Internet or through other media) seems to have led to increased occasions of negligent loss or theft of personal information stored on moveable storage systems. An informal track of personal data losses in the Europe and the US in the past three years[12] shows that millions of personal records have been lost, misplaced or stolen in often the most mundane of situations – a laptop with stored personal information of employees/clients etc. stolen when left unattended in a car; storage media left on trains; a cd with personal information (including bank records, social security numbers and other important personal identifiers) lost in the mail; banks' or shops' client information systems hacked and so on.

The Data Protection Directive and the national laws implementing it all impose an obligation on the data controller to keep the personal information collected and processed in a secure manner[13] and "to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss"[14].

While all the national legislations include this obligation, there are a number of limitations to the effectiveness of this obligation. One major limitation lies with the reduced or limited powers of Data Protection authorities to enforce this obligation and impose sanctions when this obligation is breached. For a wide variety of reasons, some Member States have chosen to give their data protection authorities very limited powers to police the implementation of the data protection obliga-

[12] See 'Table of Losses' attached to J. Cannataci, J.P. Mifsud Bonnici, *The UK 2007 Data Protection Fiasco: Moving on from Bad Policy and Bad Law,* in "International Review of Law, Computers and Technology", Vol. 23, nn. 1-2, 2009, pp. 47-76.

[13] Art 17 - Data Protection Directive.

[14] Art 17(1) - Data Protection Directive.

tions[15]. While the data protection authorities in some countries, like Italy, have relatively wide powers to inspect premises where personal information is kept by companies, in other countries such as the UK, the Information Commissioner was effectively barred from spot-checks of either the public or the private sectors. His officers could only inspect premises and records after giving advance warning and with the agreement of the civil servants or companies concerned[16].

A related limitation to inadequate enforcement is the absence of real sanctions for breaches of the obligations of this article. Data protection authorities have limited sanctions that they can apply after investigating breaches. Proper sanctions can work as incentive for data controllers (and employees within a company) to take the obligations of article 17 seriously.

The Data Protection directive (in article 23) requires that Member States provide a way for persons "who have suffered damage as a result of an unlawful processing operation or of any act incompatible"[17] with the Directive to be entitled to compensation from the controller for the damage suffered. In many national legislations, individual citizens may bring a claim of compensation under general private (or civil) law provisions[18]. Had a citizen to take such action however, the burden of proof for the damage caused by a negligent loss of a company would lie with the citizen – a burden, one may argue, that is disproportionately large.

While arguing for necessary changes to be made to the power of data protection authorities, we may also consider whether there are complementary courses of action can be followed in such cases. In this part of the paper the author explores the usefulness of using developments in

[15] Bignami argues that "compared to other areas of European law, the Data Protection Directive gives surprisingly few powers to the European network of privacy regulators; the bargaining history [she claims] shows that this decision was driven by extreme disagreement on the importance of privacy." F. BIGNAMI, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, in "Michigan Journal of International Law", Vol. 26, 2005, p. 810.

[16] J. CANNATACI, J.P. MIFSUD BONNICI, *op. cit.*

[17] Article 23 - Data Protection Directive.

[18] See for example Article 46 of the Maltese Data Protection Act (Chapter 440 of the Laws of Malta).

public international law on private sector responsibility for breaches of fundamental rights – e.g. in the case of breach of property rights or environmental rights – and the shifting of liability of private sector liability to states in cases of breaches of fundamental rights – e.g. where the state takes responsibility for breaches (of e.g. environmental protection) carried out by private companies established in its territory.

4.1. Responsibility of Non-state Actors for Human Rights Violations

There is a growing literature on the responsibility of states and non-state actors in violations of human rights[19]. Traditionally the responsibility for the protection of human rights lies with states. States have the responsibility to provide the necessary environment and laws for the protection of human rights within a state and for relevant sanction where human rights are violated. Citizens can bring actions against the state where the state alleged violates the citizens' human rights. Courts have, in most European courts reviewed actions of governments for human rights violations and citizens in Europe can, once local remedies are exhausted, bring their claims before the European Court of Human Rights. What this in fact means for our debate on protection of informational privacy, is that violations by a state or parastatal organisations of informational privacy may be brought before a court and citizens may be compensated (and/or laws changed) if the court finds for the citizen bringing the action. Numerous allegations of the violation of the right to non-infringement of one's private and family life (including protection for informational privacy) have been brought before the European Court of Human Rights[20].

While the responsibility of states for their own actions is often clear, it is not clear whether private corporate entities have enforceable obligations to protect human rights and whether states are also responsible for the actions of private corporate entities established in its territory. It is

[19] See for example, R.G. STEINHARDT, *Soft Law, Hard Markets; Competititve Self-interest and the Emergence of Human Rights Responsibilities for Multinational Corporations*, in "Brooklyn Journal of International Law", Vol. 33, 2007, pp. 933-953.

[20] E.g. Hannover v. Germany; S and Marper v. UK etc.

increasingly argued, e.g. in the environmental field, that private companies can be directly held responsible for violations of human rights (e.g. the right to property). As a response to this devolution of responsibility of human rights violations to the private sector, the private sector has in many areas developed codes of practice or standards of practices delimiting their responsibility[21]. Steinhardt argues that "one dominant critique of the corporate responsibility initiative suggests that it subverts shareholder primacy by requiring management to develop an expertise in human rights law and exercise *de facto* control over abuses …raising costs without raising revenues"[22]. Yet one can also argue that human rights are rights that every human being has *erga omnes* and not solely against his own State or another state, as guarantors of an environment of human rights' protection. No person should be allowed with impunity to breach the fundamental human rights of others.

Unlike other areas, as noted earlier, where private companies have taken what has been called an "entrepreneurial approach to human rights"[23] and have identified their human rights obligations as an industry and adopted these obligations in the standard business practices, this has not yet happened for the protection of informational privacy. Even if most businesses active online have privacy policies, none of these policies contain any provision on the remedies available to individuals if personal information kept by the company is accidentally or negligently lost or stolen.

Apart from waiting for business to take an entrepreneurial approach to human rights, one could also argue that businesses can also be held responsible for human rights violations. It has also been argued that human rights obligations are not different in kind from other sources of obligation in trade law[24]. In support of this argument is that any business can be held liable for damages caused by the negligence or intentional acts of its employees. Following this logic, negligent acts or intentional acts that violate human rights obligations should not be treated any differently.

[21] See Code of practice for diamonds - Kimberly Process Certification Scheme; for forestry etc.

[22] See R.G. STEINHARDT, *op. cit.*, p. 933.

[23] See R.G. STEINHARDT, *op. cit.*, p. 937.

[24] See R.G. STEINHARDT, *op. cit.*, p. 941.

It is legally more difficult however to claim that citizens can bring an action for damages caused by a violation of their right to informational privacy based not on data protection law but directly on the basis of fundamental rights. The question here is, are Article 8 ECHR and Articles 7 (protecting the right to private life) and 8 (protecting the right to data protection) Charter of Fundamental Rights of the European Union justiciable against private parties? Arguably (given the novelty (post coming into force of the Lisbon Treaty in December 2009)) one will first need to answer the question whether Articles 7 and 8 of the Charter of Fundamental Rights of the EU have direct effect vertically against the action of states and horizontally against the action of private actors. Following Article 6 TEU the Charter of Fundamental Rights has "the same legal value as the Treaties" and is addressed "to the Member States only when they are implementing Union law"[25]. This does not however mean that each of the fundamental rights is directly effective.

In case of Treaty provisions, the ECJ has held in *Van Gend en Loos* (and developed further in subsequent decisions such as *Van Duyn and Defrenne*) that "a Treaty Article will be accorded direct effect provided that it is intended to confer rights on individuals and that it is sufficiently clear, precise and unconditional"[26]. Whether Articles 7 and 8 satisfy these criteria is yet to be decided.

4.2. State Responsibility in Case of Non-state Actor Violation of Human Rights

Contemporaneously, there is a tendency to consider states also liable for violation of human rights by companies established in their territory. What is argued here is that states have the ultimate responsibility to protect human rights and cannot relinquish their responsibility when the violations are committed by a private company established within its territory.

What are the implications of this trend for the protection of informational privacy in cyberspace? Within this second approach – holding states

[25] Article 51(1) Charter of Fundamental Rights of the European Union OJ 2010/C 83/02.

[26] See P. Craig, G. De Burca, *EU Law: Texts, Cases and Materials*, Oxford, Oxford University Press, 2008, 275 p.

responsible for human rights violations committed by private companies – this could in practice mean that citizens' can bring human rights actions against the state when a private company would have in any way (negligent loss, theft, mishandling) misused the private information it held.

One important aspect not discussed so far is the question of jurisdiction. Collection of personal information on the Internet is, to many extents, borderless or not specifically bound to one geographical space. If one were to take as an example the social network Facebook with more than half a million users, the personal information collected from and about those users is no bound to one geographical territory. Where would a user bring an action to remedy a human rights violation? Which state can be held responsible for the breach of informational privacy by Facebook? Are the 'traditional' of jurisdiction – e.g. territorial or personal link between the dispute and the jurisdiction of the court – enough? And what *law* should apply? Given the universality of human rights one would argue that the choice of law problem should not arise here. However, given that the right to informational privacy is only unambiguously identified as a fundamental right in the EU Charter of Fundamental Rights, the universal aspect of the human right might come into question. There is a possibility that state courts take a parochial approach, preferring a narrow interpretation of jurisdiction, preferring their own jurisdiction over possibly the jurisdiction of other courts and preferring their restrictive interpretation on the possibilities of holding states and private actors liable for human rights violations. This uncertainty on jurisdiction acts against citizens as it offers no clear route to avail themselves of possible (possibly also undetermined) remedies.

5. Scenario 2: Mergers and Acquisitions

The second situation to be considered here is the following: similar to business enterprises active off-line, businesses online often merge or are bought-off by other businesses. In these business transactions personal information of clients or employees etc. coming from the different businesses are also merged. Combining already large collections of personal information in a reality where so much can be done with the personal information can be considered to be another threat to personal informational privacy unless appropriate safeguards are in place.

In the current data protection legislation structure there is no method to forestall situations or impose specific protections where a commercial entity in the course of its transactions with other commercial entities (e.g. during a merger or take-over) increases its store of consumer personal data. The urgency of adequate protection of consumer information becomes even more acute when two online companies merge giving one company exceptionally wide access to consumer information, as in the Google-DoubleClick merger in 2007 where it was argued that the acquisition of DoubleClick would permit Google to have more information about the Internet activities of consumers than any other company in the world[27]. Data protection legislation would need to be followed after the merger but there is no means in the legislation to impose specific safeguards to ensure that the personal information would not be exploited in a way to threaten consumer privacy[28].

Under fair competition/antitrust rules, a merger can be reviewed by the EU Commission in Europe and the Federal Trade Commission (FTC) in the United States to establish whether the merger could potentially constitute unfair and deceptive trade practices. Could one of the review criteria be the potential threats of privacy by the concentration of too much consumer information in the control of one corporate entity?

There is a growing trend (seen particularly in the US[29]) to attempt to include privacy concerns in anti-trust/unfair competition proceedings. Indeed in 2007, the Google-DoubleClick merger was challenged by a number of organisations in the US on privacy and antitrust grounds[30].

[27] EPIC complaint to the FTC April 2007, available at http://www.epic.org/privacy/ftc/google/epic_complaint.pdf.

[28] One can argue that if information has been supplied to a particular company on trust and for the purposes informed of at the moment of collection, it would not only be a major breach of trust if that information is passed to another but also a breach of data protection obligations (to process and keep personal information only for specified purposes).

[29] See for example Geocities case in 1999 - "In the matter of Geocities, Agreement Containing Consent Order, File No. 9823015 (12 February 1999) (available at http://www.ftc.gov/os/1998/08/geo-ord.htm) and ToySmart.com in 2000 (available at http://www.ftc.gov/opa/2000/07/toysmart2.shtm).

[30] The Electronic Privacy Information Center (EPIC) file a complaint on 20 April 2007 with the Federal Trade Commission requesting the FTC to (a) issue an injunction to prevent

Access to personal information of consumers was also one of the concerns investigated by the EU Commission in the proceedings examining whether the merger would significantly impede fair competition[31]. Both the US Federal Trade Commission and the EU Commission eventually found that there was no situation of distortion of competition by the merger and authorised the merger to proceed. This notwithstanding, this case (and others) has given rise to increased awareness of the possibility of using competition (and anti-trust) principles to protect individuals' informational privacy. One can question however whether competition and anti-trust principles are in fact appropriate mechanisms to be used in the protection of consumer personal information privacy.

5.1. Personal Information as a Commercial Asset

As pointed out in the beginning of this paper thanks to the advances in information technology is it relatively easy and cheap for companies to amass personal consumer information. Thinking in market terms, the ease with which personal consumer information can be collected produces a steady supply of personal information which is taken up by companies that increasingly consider large data sets of consumer information as essential assets for companies trading online. By using consumer information, companies can tailor their goods and services to match the preferences and dislikes of the market. One can expect that a company with a wide and large data set of consumer information can have a competitive edge over other competitors who may have lesser stores of personal data. Having large sets of personal information could also be exploited in a way that threatens consumers' privacy.

the merger and (b) to conduct an investigation regarding the circumstances of the merger. The complaint alleged that "the acquisition of DoubleClick will permit Google to track both a person's Internet searches and a person's web site visit...giv[ing] one company access to more information about the Internet activities of consumers than any other company in the world. Moreover, Google will operate with virtually no legal obligation to ensure that privacy, security and accuracy of the personal data that it collects", available at http://www.epic.org/privacy/ftc/google/epic_complaint.pdf.

[31] COMMISSION DECISION of 11/03/2008 declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement (Case No COMP/M.4731 - Google/DoubleClick) C(2008) 927, available at http://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf.

The personal information market is not quite as perfect as it seems with supply and demand keeping each other in check. The market is not transparent: the original supplier of the person information (the data subject) has little or no control over the use of the personal information supplied. Data protection legislation in Europe tries to address this lack of transparency by requiring consent of the data subject and that the data subject is informed of the purpose of collection and use of the personal information. Theoretically at least, the giving of information allows the data subject/consumer to then make informed choices about the use of his/her personal information. As in other areas of consumer law, where the notion of informed consumer is central[32], there are limits to the effectiveness of this obligation as a remedy against abusive use of personal information. One could argue that companies in a leading position in the market may potentially afford to ignore traditional privacy safeguards (where they exist at all). The difference between companies abiding with data protection or other privacy legislation and those which do not can also result in the non-abiders having a competitive edge on competitors following the more onerous obligations of privacy protection. Data protection legislation does not provide remedies to balance the inequality between abiders and non-abiders with the laws. Furthermore, where the reach of European data protection law does not reach (or is ignored), the consumer is left in an even more vulnerable position with his/her personal information being traded while he/she has little power over the use of personal information.

There is a growing school of thought[33] that law should grant the data subject/consumer a property right in their own personal data and be

[32] See for example, T. WILHELMSSON, *The Informed Consumer v the Vulnerable Consumer in European Unfair Commercial Practices Law - A Comment*, In Howells G., Twigg-Flesner C., Parry D., Nordhausen A., "The Yearbook of Consumer Law 2007", United Kingdom, Ashgate Publishing, Ltd., 2007 and S. WEATHERILL, *The Rôle of the Informed Consumer in EC Law and Policy*, in "Consumer Law Journal", Vol. 2, 1997, p. 49.

[33] See for example P. SAMUELSON, *Privacy as Intellectual Property?* In "Stanford Law Review", Vol. 52, 2000, p. 1125 and E. DOMMERING, *Van 'Ja zuster, nee zuster' naar 'Discodans': de lange weg naar commerciële informationele privacy*, in Visser D.J.G. (ed.), "Commercieel portretrecht 't Schaep met de 5 pooten", Netherlands, Uitgeverij deLex, 2009, pp. 259-273.

allowed to negotiate with business which personal data to reveal to which firms for what purposes and for what price. This approach assumes a move towards a market-based approach rather than a fundamental rights approach which has so far dominated European thinking. While a property rights model has some appeal in (theoretically at least empowering the consumer), it is hard so far to imagine its viability in practice and its prospect of achieving information privacy goals[34].

5.2. Competition Law

The regulation of mergers between business entities falls under a different area of law to privacy law: competition law (or antitrust law in the US). *Prima facie*, the aims of competition law have little in common with (if not antithetical to) the concerns privacy law seeks to address. In essence competition law has three elements: a. prohibiting agreements or practices that restrict free trading and competition between business entities; b. prohibiting abusive behaviour by an entity dominating a market or practices that tend to lead to a dominant position; and c. supervision of mergers and acquisitions of entities. The main enforcement entity for fair competition/antitrust rules at a European level is the EU Commission and the Federal Trade Commission (FTC) is the equivalent entity in the United States.

In theory, by applying competition policy ensuring that companies compete with each other in a free and fair manner while offering their goods and services, consumers are also being offered better services and goods. It is often argued[35] that the end beneficiary of fair market rules is the consumer (even if the rules as such do not mention consumers or consumer protection).

Given that consumer protection is a goal shared by both privacy law and competition policy, and given the evident commercial value of personal information in today's online trading businesses, there is a growing

[34] See SAMUELSON, *op. cit.* p. 1125 for an eloquent discussion on the viability and difficulties of such a system.

[35] See for example E. EDWARDS, *Stepping up to the Plate: the Google-DoubleClick Merger and the Role of the Federal Trade Commission in Protecting Online Data Privacy,* 2008, available at SSRN http://ssrn.com/abstract=1370734.

trend (seen particularly in the US[36]) to attempt to include privacy concerns in anti-trust/unfair competition proceedings. There is yet no comprehensive research identifying the role competition policy mechanisms can play (if at all) in the protection of personal informational privacy.

On the one hand it can be argued that competition policy mechanisms play no role in the protection personal informational privacy simply because competition policy is geared towards the regulation of economic factors and not non-economic factors like privacy protection. This position can be defended through economics-based competition analysis, inspired by the so-called "Chicago School" of competition theory that shows that "non-economic" factors, including privacy protection, are best dealt with by legislation and not by competition policy.

On the other hand, it can also be argued that since there is a market for personal information, personal privacy should be framed in market terms and no longer, solely, from a fundamental rights perspective. Following then a market-driven approach to privacy protection, one could argue that privacy protection is so fundamental that there should be an obligation to integrate privacy protection in all regulation and policies, including competition policy.

What one can definitely see however, from the handling of the Google-DoubleClick merger examination, is that while competition policy has mechanisms that can be used to protect personal privacy, integrating privacy matters in the current competition law enforcement structure will need some institutional and cultural changes to happen[37].

Despite the length of time to instigate and wait for the necessary changes to happen, it is important that interested organisations or individuals continue to challenge mergers and acquisitions of companies having access to broad collections of personal information. The mere process of asking for review can achieve safeguards that consumers would not have otherwise had. An example of this can be seen in the

[36] See for example Geocities case in 1999 - "In the matter of Geocities, Agreement Containing Consent Order, File No. 9823015 (12 February 1999) (available at http://www.ftc.gov/os/1998/08/geo-ord.htm) and ToySmart.com in 2000 (available at http://www.ftc.gov/opa/2000/07/toysmart2.shtm).

[37] See E. EDWARDS, *op. cit.*

DoubleClick-Abacus Direct acquisition in 2000. When DoubleClick (an Internet advertising company) purchased Abacus Direct (a market research company), the acquisition also sparked concern that consumer privacy may also be harmed by the transaction. Ultimately, a consent decree maintaining the separation between the consumer databases was awarded, securing to some degree consumers' informational privacy[38].

6. Conclusion

In a world where online providers seek to convince their customers that 'privacy is dead' in an attempt to enjoy *carte blanche* over the personal information they collect, discussing safeguards and remedies for informational privacy takes on a renewed appeal. It is important for consumers to appreciate that there are viable mechanisms that can be invoked to protect one's personal information.

With "private enterprises now control[ing] more powerful resources of information technology than ever before"[39] is it important to review the current legal framework protecting informational privacy. This paper has looked at two specific scenarios where consumers' rights to information privacy may be violated, considering the limits of the current data protection legislation and the possibility of using other fields of law to complement the current framework of protection.

In the first scenario – involving situations of possible negligent loss or theft of personal information – one can see that while the current legal framework (set by Directive 95/46/EC) sets an obligation for data controllers to use appropriate mechanisms and institutional setups to secure personsal information, the law stops short from giving the data protection enforcement authorities enough power to ensure compliance with the obligation by data controllers. While a first recommendation is to encourage necessary changes to the law, the paper also explored other

[38] R. Hahn, H.J. Singer, *An Anti-trust Analysis of Google's Proposed Acquisition of Double Click*, 2008, accessed at SSRN http://ssrn.com/abstract=1016189.

[39] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, in 52 Vand. L. Rev. 1609, 1633 (1999) as cited in D. Solove, *A Brief History of Information Privacy Law*, in "Proskauer on Privacy", pp. 1-46, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id =914271.

possible remedies for consumers. It looked at the responsibility of non-state actors for the violation of human rights and state responsibility for non-state actor violations. The routes offered basing one's claims on the direct responsibility of non-state actors for violations of information privacy or of claiming state responsibility for non-state actor violations may exist but still need to be tested before a court of law.

In the second scenario – involving mergers and acquisitions of companies holding large collections of personal information – the route explored in this paper, of using FTC and EU Commission anti-trust scrutiny mechanisms, has already be used in practice. Although the current outcomes have been limited, it is, highly unlikely that these mechanisms are not used again in future mergers of key industry players. As Edwards argues "despite the view of traditional analysts and observers, the FTC [and the EU Commission] has the authority to analyze data privacy issues, where appropriate, as part of its merger review"[40]. It is a matter of more detailed study, as well as persuading the FTC and EU Commission, and then mustering the political will to provide for better protection of informational privacy.

Ultimately what this article aims to show is that consumers can benefit from better data protection legislation safeguards complemented by developments going in linking human rights violations by the private sector to states and to the experimental field of using competition law structures to protect citizens' informational privacy online.

[40] E. EDWARDS, *op. cit.*

Privacy e *design*

UGO PAGALLO*

SOMMARIO: *1. Introduzione – 2. Teoria giuridica del* design *– 3. Il* design *nella protezione dei dati personali – 4. La posta in gioco tra informatica e diritto – 5. Conclusioni*

1. INTRODUZIONE

Nella prima edizione di *The Sciences of Artificial*, pubblicato per i tipi della MIT Press nel 1969, Herbert A. Simon lamentava lo stato di abbandono, teoretico e accademico, in cui versava la "scienza del *design*"[1]. A giudizio del futuro premio Nobel, "rispetto alle norme prevalenti, la rispettabilità accademica esige che le materie trattate debbano essere intellettualmente robuste, analitiche, formalizzabili ed insegnabili. Nel passato, molto, se non la maggior parte, di ciò che sapevamo attorno al *design* e le scienze artificiali era intellettualmente sommesso, intuitivo, informale e artigianale"[2].

Trent'anni dopo, in *Code and Other Laws of Cyberspace*, era il turno di Lawrence Lessig per stigmatizzare il fatto che, malgrado il ruolo cruciale svolto dall'architettura, o "codice", nel perseguimento di finalità sociali o collettive, i giuristi avessero per lo più riservato scarsa attenzione all'impatto del *design* nei rapporti intersoggettivi[3].

Molta acqua, da allora, è passata sotto i ponti.

Innanzitutto, lo stesso Simon ricorda nella terza edizione di *The Sciences of Artificial* (1996), come, a partire dalla metà degli anni settanta, con la fondazione del *Design Research Center* presso la Carnegie Mellon University, sia venuta emergendo e consolidandosi una vera e propria "scienza del *design*". "In sostanza, la teoria del design mira ad ampliare le capacità dei

* L'Autore è professore ordinario di Filosofia del diritto alla Facoltà di Giurisprudenza dell'Università di Torino, Faculty del Center for Transnational Legal Studies di Londra.

[1] Il richiamo va sin d'ora alla terza edizione di H.A. SIMON, *The Sciences of Artificial*, Cambridge, Mass.-London, MIT Press, 1996. Si tenga presente che, sempre nel 1969, appariva la prima edizione di N. POTTER, *What Is a Designer*, London, Hyphen Press, 2002.

[2] H. A. SIMON, *The Sciences of Artificial*, cit., p. 112.

[3] Si v. infatti L. LESSIG, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999, pp. 91-92.

computer nel dare aiuto al design, attingendo ai mezzi della intelligenza artificiale e della ricerca operativa"[4].

Nel frattempo, è venuta del pari maturando la consapevolezza dei giuristi, nonché dei legislatori e autorità garanti in materia di tutela dei dati personali, a proposito del ruolo svolto dal *design* sul piano delle relazioni intersoggettive. Dopo il fugace richiamo nel considerando 46 della direttiva 95/46/CE – dove il termine *design* è reso nella versione italiana come "momento della progettazione" – la formula *privacy by design* è stata coniata alla fine degli anni novanta dal Commissario per la *privacy* dell'Ontario, in Canada, Ann Cavoukian. La formula, poco più tardi, sarebbe stata ripresa in alcuni testi ufficiali, tra cui il *Privacy Design Principles for an Integrated Justice System* presentato, nell'aprile 2000, dal Dipartimento della giustizia nordamericano e dal Commissario per la *privacy* dell'Ontario. Più di recente, il 1° dicembre 2009, il Gruppo di lavoro *ex* art. 29 D-95/46/CE, insieme al Gruppo di lavoro per la polizia e la giustizia, ha pubblicato un documento su "Il Futuro della Privacy", in cui viene dato ampio spazio, appunto, al "nuovo principio della *privacy by design*".

Il crescente interesse dei giuristi per i temi (informatici) del *design*, specie in materia di tutela e trattamento dei dati personali, rischia tuttavia di ingenerare un equivoco. Secondo il titolo del presente saggio e come già capitato ad altri e ben più autorevoli scritti – penso solo a *Verità e metodo* di Hans-Georg Gadamer, o a *Dio e stato* di Hans Kelsen – bisogna infatti stabilire se la "e" del rapporto tra *privacy* e *design* abbia un senso congiuntivo o disgiuntivo. Se, cioè, si propugni la tutela della *privacy* come *design* o il *design* come una modalità di tutela dei dati personali.

Al fine di chiarire i termini della questione, il presente saggio è suddiviso in quattro parti.

In primo luogo, illustro i termini generali del problema, vale a dire come il *design* incida sul fenomeno giuridico e sulla disciplina delle relazioni intersoggettive.

Secondariamente, spiego come le prospettive in tema di *design* siano state in concreto declinate in materia di tutela dei dati personali.

[4] H.A. SIMON, *The Sciences of Artificial*, cit., p. 114.

Quindi, esamino sia le tesi sulla *privacy* come *design* sia quelle del *design* come *una* modalità di tutela nel trattamento dei dati personali.

Dopo di che, sarà giunto il momento di trarre le conclusioni.

2. Teoria giuridica del *design*

È stato indubbiamente merito di Lessig aver attirato l'attenzione dei giuristi sui modi in cui il *design* determini e/o condizioni il comportamento dei soggetti, sia nel mondo reale sia nel mondo virtuale di internet[5].

Per quanto riguarda il mondo reale, è sufficiente menzionare i ponti di Long Island, costruiti in modo da bloccare il transito degli autobus, oppure l'impiego dei dossi nei fondi stradali per ridurre la velocità delle automobili (dossi che, con la consueta sagacia tropicale, sono soprannominati in Venezuela "poliziotti sdraiati"). Per quanto attiene al mondo virtuale di Internet, si rifletta invece sui "codici" TCP/IP e http, nell'intreccio con questioni di anonimato in rete e *spamming*, oltre ai temi relativi alla tutela del *copyright* con l'uso di DRM (*Digital Rights Management*).

Ulteriori ricerche sono state condotte nell'ambito del diritto penale[6], dell'architettura di Internet e del suo impatto sul piano delle garanzie costituzionali[7], e via dicendo.

Ma, si deve forse a Karen Yeung il primo tentativo di elaborare una compiuta teoria generale del *design* in ambito giuridico[8].

In questa sede, possiamo concentrarci sui due aspetti più rilevanti della tassonomia proposta.

[5] Cfr. L. Lessig, *Code and Other Laws*, cit., pp. 90-98.

[6] Si v. ad esempio N.K. Katyal, *Architecture as Crime Control*, in "Yale Law Journal", 2002, 111, pp. 1039-1139; nonché Id., *Digital Architecture as Crime Control*, in "Yale Law Journal", 2003, 112, pp. 101-129.

[7] J. Zittrain, *The Future of the Internet and How to Stop It*, New Haven, CT, Yale University Press, 2008.

[8] Cfr. K. Yeung, *Towards an Understanding of Regulation by Design*, in Brownsword R., Yeung K. (eds.), "Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes", London, Hart Publishing, 2007, pp. 79-108. In questa sede possiamo lasciare in parentesi altre utili suddivisioni come, ad esempio, quella proposta da N. Potter, *What Is a Designer*, cit., p. 4, per cui occorre distinguere tra oggetti (*design* di prodotto), luoghi (*design* ambientale) e, infine, messaggi (*design* di comunicazione).

In primo luogo, occorre prestare attenzione all'*oggetto* che volta per volta si regola attraverso uno specifico *design*: la progettazione può infatti riguardare non solo spazi e luoghi (i ponti di Long Island o i dossi stradali ricordati precedentemente), oppure prodotti e processi produttivi (come nel caso dei DRM). In realtà, il *design* concerne anche la riconfigurazione di organismi viventi come piante, animali ed esseri umani: nell'ordine, è il caso degli OGM, dei salmoni geneticamente modificati e di tutto l'odierno dibattito in tema di post-umano e *cyborgs*.

In secondo luogo, bisogna far caso alle stesse *modalità* del *design*: la progettazione può avere il fine di modificare il comportamento dei soggetti, oppure, di ridurre l'impatto di eventi dannosi o, infine, di prevenire del tutto la possibilità che quel presunto evento dannoso si verifichi.

Per illustrare la prima ipotesi, è sufficiente tornare al *design* dei dossi come forma per invogliare un comportamento più prudente: perfino il più incallito automobilista italiano emulo di Alonso dovrebbe pensarci su due volte prima di sfrecciare a centoventi in una strada nella quale egli sa che corre il rischio di sfasciare la propria macchina!

Quanto alla seconda modalità di *design* e rimanendo nell'universo delle automobili, basti citare l'*air-bag*.

Infine, rispetto all'obiettivo di garantire una prevenzione totale tramite *design*, è sufficiente menzionare le macchine intelligenti in grado di arrestarsi o ridurre la velocità a seconda che siate stanchi o ubriachi oppure delle congiunture dell'ambiente circostante[9].

Delle nove combinazioni possibili proposte dallo schema, quali, dunque, i casi più pertinenti al tema della *privacy* e *design*? Esclusi, va da sé, i casi di progettazione su piante e animali come i salmoni geneticamente modificati, quali le ipotesi più interessanti riguardo al trattamento e tutela dei dati personali?

[9] Lungi dall'essere un mero esempio di *science fiction*, segnalo al lettore che su questi temi va lavorando la Cattedra UNESCO in "*data privacy* e comunicazioni macchina-macchina" presso Tarragona, in Spagna. Oltre alle pubblicazioni in rete di Josep Domingo-Ferrer, si v. la sua comunicazione *The "Backwards, Forwards and Sideways" Changes of ICT*, in Arias-Oliva M., Bynum T.W., Rogerson S., Torres-Corona T. (eds.), "ETHICOMP 2010", Tarragona, URV, 2010.

3. Il *DESIGN* nella protezione dei dati personali

Nei lavori di Ann Cavoukian, alla quale dobbiamo, forse, non solo la formula *privacy by design* ma altresì quella di PETs ossia *Privacy Enhancing Technologies*, troviamo una guida efficace per cominciare a chiarire il rapporto tra *privacy* e, appunto, *design*[10].

In sostanza, l'idea è che le misure a tutela della *privacy* debbano essere presenti sin dalla fase di progettazione degli strumenti preposti al trattamento ed elaborazione dei dati, affinché, secondo il principio di minimizzazione, tali sistemi possano raccogliere, processare e utilizzare la minore quantità possibile o, se del caso, nessun tipo di dato personale. Con gli esempi proposti dai Gruppi di lavoro comunitari[11], si pensi ai sistemi di video-sorveglianza nel settore dei trasporti pubblici, che dovrebbero essere progettati in modo tale da non permettere il riconoscimento dei volti (salvo, ovviamente, per il caso di delitti); oppure, si considerino i sistemi di elaborazione dei dati negli ospedali, in cui i nomi dei pazienti ed altri elementi identificativi dovrebbero essere tenuti rigorosamente separati dai dati sullo stato di salute e relativi trattamenti medici.

Oltre al rispetto del principio di minimizzazione, i sistemi per la raccolta e il trattamento dei dati dovrebbero essere progettati al fine di garantire l'effettivo controllo degli interessati sui propri dati personali, di pari passo con la trasparenza del sistema, vale a dire che i titolari dei dati possano essere sufficientemente informati sulle modalità operative del sistema stesso. Ad esempio, il disegno degli interfaccia informatici dovrebbe essere "intuitivo" per l'utente o, come suole dirsi, *user friendly*. Tra i vari meccanismi, è il caso dell'inserimento di collegamenti semplici ed efficaci per la richiesta d'informazioni o l'inoltro di reclami da parte degli utenti, impostando al contempo il sistema in modo tale che la minimizzazione della raccolta e la condivisione dei dati avvengano, specie nei servizi di *social network*, per *default*[12].

[10] Cfr. A. Cavoukian, *Privacy by Design*, Ottawa, IPC Publications, 2009.

[11] Si v. il documento, presentato il 1° dicembre 2009 dal Gruppo di lavoro *ex* art. 29 D-95/46/CE e dal Gruppo di lavoro per la polizia e la giustizia, "Il Futuro della Privacy" – 02356/09/EN WP 168, specie parr. 44-53.

[12] La questione, sollevata dal Gruppo di lavoro *ex* art. 29 nell'Opinione 5 del 12 giugno 2009 (01189/09/EN - WP 163), è stata al centro del convegno su *Intelligent Privacy*

Tra i vari approcci informatici, una particolare menzione va fatta al settore delle ontologie giuridiche[13]. L'obiettivo di questi sistemi consiste infatti nel rappresentare la conoscenza *iuris et de iure* con la formalizzazione dei concetti tradizionalmente impiegati dai giuristi – come norme, diritti o doveri – affinché una macchina possa comprendere e processare tale informazione. Distinguendo i compiti tra le ontologie che elaborano tutti i concetti più rilevanti del dominio interessato con l'uso di tassonomie, e le ontologie che includono le sole regole e restrizioni concernenti quello stesso dominio, l'obiettivo è di offrire maggiori garanzie nelle fasi di accesso, conservazione, gestione e uso degli archivi informatici contenenti dati personali, automatizzando i processi di tutela e trattamento di quei dati.

Naturalmente, gli accorgimenti a tutela della *privacy* non soltanto riguardano il *design* dei prodotti o dei processi produttivi. Come ricordato dai Garanti europei nel parere su "Il Futuro della Privacy", sarebbe opportuno che gli strumenti di identificazione biometrica non rinviino alle informazioni contenute in banche dati ma, sotto forma di *smart card*, che tali dati siano piuttosto tenuti sotto il diretto controllo degli interessati.

Tuttavia, che dire sulle finalità di questi accorgimenti? Si tratta di trasformare il comportamento dei soggetti e ridurre il rischio che accadano eventi dannosi? E se invece l'idea fosse quella di eliminare alla radice la stessa possibilità che quell'evento dannoso accada?

A ben vedere, è proprio quest'ultimo il punto principale che finisce per dividere spesso il parere di politici ed esperti. Attraverso le accortezze del *design*, si mira a rendere effettivo il quadro normativo e le sanzioni previ-

Management Symposium, organizzato presso l'Università di Stanford, CA., il 22-24 marzo 2010, cui hanno partecipato alcuni dei giganti del settore quali Google, Facebook, Apple, ecc. Il programma su http://research.it.uts.edu.au/magic/privacy2010/.

[13] Si v. ad esempio D. ABOU-TAIR e S. BERLIK, *An Ontology-based Approach for Managing and Maintaining Privacy in Information Systems*, in "Lectures notes in computer science", Heidelberg, Springer, 2006, n. 4275, pp. 983-994; H. MITRE, A. GONZALEZ-TABLAS, B. RAMOS, A. RIBAGONDA, *A Legal Ontology to Support Privacy Preservation in Location-based Services*, in "Lecture notes in computer science", Heidelberg, Springer, 2006, n. 4278, pp. 1755-1764; nonché G. LIOUKADIS, G. LIOUDAKISA, E. KOUTSOLOUKASA, N. TSELIKASA, S. KAPELLAKIA, G. PREZERAKOSA, D. KAKLAMANIA, I. VENIERISA, *A Middleware Architecture for Privacy Protection*, in "The International Journal of Computer and Telecommunications Networking", 2007, 51(16), pp. 4679-4696.

ste dai legislatori competenti, come suggerito dalle Autorità garanti per la *privacy* in Europa, oppure, come propende il Commissario per la *privacy* in Ontario, è forse il caso di sostituire progressivamente quelle norme e sanzioni, spesso del tutto inefficaci, con automatismi tecnici?

4. La posta in gioco tra informatica e diritto

La concreta possibilità di automatizzare molti meccanismi di tutela a presidio della *privacy* sembra per molti versi auspicabile, tenuto conto dei problemi, non solo tecnici ma latamente culturali, sorti con l'impiego delle nuove tecnologie dell'informazione e della comunicazione (ICT). Per dirla con le stesse Autorità garanti europee, "gli utenti dei servizi di ICT – dal business al settore pubblico e certamente gli individui – non sono in condizione di assumere da soli rilevanti misure di sicurezza al fine di proteggere i dati personali propri o di altri soggetti. Ne consegue che tali servizi e tecnologie dovrebbero essere progettati [*designed*] implementando la *privacy* per *default*"[14].

Gli automatismi a presidio della *privacy*, d'altra parte, sembrano in grado di far fronte a molte delle deficienze caratterizzanti l'odierno stato dell'arte sia nel limitare la discrezionalità dei burocrati, riguardo al ri-uso della informazione nel settore pubblico, sia, come riferisco nel prossimo paragrafo, per quanto concerne le questioni di competenza e giurisdizione[15].

Di fronte al progresso tecnologico, non di meno, sussistono fondati motivi di perplessità rispetto all'ipotesi di automatizzare l'applicazione della legge, fino al punto da renderla "perfetta" a fini di prevenzione. Secondo il giudizio di Jonathan Zittrain, "la perfetta applicabilità [della legge] fa svanire la pubblica comprensione del diritto in quanto la sua applicazione [automatica] elimina un utile interfaccia tra i termini della legge e la sua imposizione. Parte di ciò che ci rende umani sono le scelte che facciamo ogni giorno su quel che rappresenta alcunché di giusto o

[14] Si v. il par. 45 del più volte citato documento su "Il Futuro della Privacy".

[15] Me ne sono ampiamente occupato in *Sul principio di responsabilità giuridica in rete*, in "Il diritto dell'informazione e dell'informatica", XXV, n. 4-5, 2009, pp. 705-734, nonché, con E. Bassi, in *The Future of the EU Working Parties' "The Future of Privacy" and the Principle of Privacy by Design*, in Bottis M. (ed.), "Proceedings of the Third International Seminar on Information Law" (Corfù, 24-25 giugno 2010), INSEIT (in corso di pubblicazione).

sbagliato (…). In un ambiente monitorato e sorvegliato del tutto, quelle stesse scelte svaniscono"[16].

Oltre a motivi di natura morale e filosofico-giuridica, ci sono poi questioni prettamente pratiche che finiscono per incidere sulle scelte politiche di fondo. Come ricorda Karen Yeung, "non solo è inevitabile il rischio di fallimenti operativi, ma la finalità di disegnare standard che siano in grado di raggiungere l'obiettivo desiderato dal regolatore in forma precisa e accurata, non può che essere, con ogni evenienza, un'impresa improba"[17]. La ragione la spiega esaurientemente uno dei massimi esperti del settore, Eugene Spafford: "L'unico sistema [informatico] realmente sicuro è quello che sia stato spento, messo dentro a un blocco di cemento e sigillato a piombo in una stanza attorniata da guardie giurate – e anche così avrei i miei dubbi"[18].

Del resto, ritroviamo con Spafford alcuni dei problemi emersi con le ricerche di ontologie giuridiche di cui al paragrafo precedente[19].

La formalizzazione delle disposizioni normative in materia di tutela dei dati personali non solo ha a che fare con nozioni rigorosamente definibili in termini di ruoli, processi o relazioni, come ad esempio avviene con le tradizionali categorie dell'obbligo, del divieto o del permesso. Molti dei concetti chiave in tema di *privacy* dipendono strettamente dal contesto in cui essi vanno inseriti: a partire dall'idea di dato personale, basta far caso alla definizione di "responsabile del trattamento" che, a giudizio del Gruppo di lavoro *ex* art. 29 D-95/46/CE, deve essere inteso come "un concetto funzionale, volto a stabilire le responsabilità in rapporto alle circostanze del caso e, per ciò, basato su un'analisi di tipo fattuale più che di stampo analitico"[20].

[16] Cfr. J. ZITTRAIN, *Perfect Enforcement on Tomorrow's Internet*, in Brownsword R., Yeung K., "Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes", London, Hart Publishing, 2007, pp. 125-156.

[17] K. YEUNG, *Towards an Understanding of Regulation by Design*, cit., p. 106.

[18] S. GARFINKEL, G. SPAFFORD, *Web Security & Commerce*, Sebastopol, O'Reilly, 1997, p. 9.

[19] Un quadro d'assieme nell'*Introduzione* a Breuker J., Casanovas P., Klein M.C.A., Francesconi E. (eds.), "Law, Ontologies and the Semantic Web: Channelling the Legal Information Flood", Amsterdam, IOS Press, 2008, specie pp. 12-14.

[20] Si v. l'Opinione 1, adottata il 16 febbraio 2010, sui concetti di "controllore" e "processore" (00264/10/EN – WP 169), p. 9.

L'obiettiva difficoltà di formalizzare alcuni concetti cardine della disciplina ha per ciò consigliato di adottare una strategia "dal basso verso l'alto" che, individuando soluzioni per classi di sotto-problemi nonché per specifiche attuazioni della normativa, possa approdare per gradi a un approccio globale della materia[21].

Più in dettaglio, la procedura prevede che, dopo la fase preparatoria relativa all'individuazione dei requisiti ontologico-giuridici relativi al campo prescelto, segua la fase di sviluppo del progetto con l'acquisizione della conoscenza tramite il sapere degli esperti, con l'inserimento dei documenti normativi e il possibile riutilizzo delle informazioni. La formalizzazione in classi, relazioni, proprietà e casi del modello dovrà poi essere sottoposta nuovamente al parere degli esperti e, infine, testata nella fase di valutazione del modello stesso attraverso l'analisi della consistenza interna e la verifica empirica che Herbert A. Simon illustrava come "ciclo del test dinamico"[22].

Come ben si vede, siamo ben lungi dalle tentazioni di garantire una "perfetta applicazione della legge"; almeno nell'ambito della tutela e protezione dei dati personali, l'alternativa secca tra la *privacy* come *design* e il *design* come una modalità di attuazione della legge, appare allo stato astratta e pure fuorviante. I timori per una "applicabilità automatica" della legge si traducono, più prosaicamente, nell'odierno dibattito sull'impostazione dei servizi di Google Buzz e, cioè, se lo scambio dei dati e informazioni debba avere per *default* natura "pubblica" o "privata"[23].

L'intenzione non è però di suggerire, attraverso le difficoltà cui vanno incontro le ricerche sulle ontologie giuridiche applicate alla *privacy*, un

[21] La difficoltà non rileva naturalmente nel solo ambito della tutela dei dati o per gli approcci dell'ontologia giuridica ma, piuttosto, in linea generale, dipende dalla necessità di ridurre la complessità informativa di sistemi, come quelli giuridici, soggetti a evoluzione nei propri concetti e rapporti. Me ne occupo in *As Law Goes By: Topology, Ontology, Evolution*, in Casanovas P., Pagallo U., Sartor G., Ajani G. (eds.), "AI Approaches to the Complexity of Legal Systems", Heidelberg, Springer, 2010, pp. 5-11.

[22] Cfr. H.A. SIMON, *The Sciences of Artificial*, cit., pp. 128-130.

[23] Si v. infatti la lettera aperta che, lo scorso 19 aprile 2010, il Commissario per la *privacy* in Canada, Jennifer Stoddart, insieme alle Autorità Garanti di Francia, Germania, Israele, Italia, Irlanda, Nuova Zelanda, Olanda, Regno Unito e Spagna, hanno mandato al capo esecutivo di Google, Eric Schmidt, a proposito delle nuove questioni di tutela dei dati personali sollevate da Buzz.

salomonico compromesso per cui il tradizionale apparato repressivo della legge andrebbe integrato con la progressiva estensione degli ambiti affidati all'automatismo tecnologico. Piuttosto, i limiti dell'odierna tecnologia con i suoi sistemi esperti invitano a riflettere sui vicoli ciechi che affliggono, nell'odierna società dell'informazione, la canonica rappresentazione del diritto come insieme di comandi suffragati da sanzioni fisiche.

In sede conclusiva, occorre ritornare al caso chiave dei conflitti di competenza e giurisdizione cui si è fatto cenno in precedenza.

5. Conclusioni

Tra i profili giuridici più rilevanti della "rivoluzione informatica"[24], spicca il fatto che quanto per secoli era l'eccezione, sta diventando la regola, ovvero che eventi e transazioni tra individui finiscano per avere sempre, virtualmente, natura e carattere transnazionali[25].

Nel caso della tutela dei dati personali, un esempio lampante per mostrare cosa ciò significhi sul piano delle garanzie e competenze giurisdizionali, è dato dai *cookie*, vale a dire i *file* di testo posti sul disco rigido del vostro computer da parte dei siti *web* che state per lo più visitando nel navigare in Internet. Provate soltanto a disattivare la funzione *default* del vostro apparecchio!

Sin dal 30 maggio 2002, con il documento 5035/01/IT – WP 56, il Gruppo di lavoro *ex* art. 29 D-95/46/CE ha avanzato la tesi che l'uso dei *cookie* debba essere inteso alla stregua degli "strumenti" previsti dall'art. 4.1(c) della predetta normativa comunitaria. Se l'obiettivo dichiarato è di "garantire che una persona non sia priva di tutela per quanto riguarda il trattamento effettuato nel suo paese per il solo fatto che il responsabile non è stabilito sul territorio comunitario", la tesi, nondimeno, finisce per confliggere sia con la lettera che con lo spirito della direttiva, conducen-

[24] Cfr. T.W. Bynum, *Introduzione* a Floridi L., "Infosfera. Etica e filosofia nell'età dell'informazione", Torino, Giappichelli, 2009.

[25] Il punto è stato segnalato con forza, ormai due lustri or sono, da David Post nella sua critica alle tesi tradizionali di Jack Goldsmith sul diritto internazionale pubblico e privato. Si v. J. Goldsmith, *Against Cybernarchy*, in "University of Chicago Law Review", 1998, 65, pp. 1199-1250; e D. Post, *Against "Against Cyberanarchy"*, in "Berkeley Technological Law Review", 2002, 17, pp. 1365-1383.

do a esiti paradossali: le giurisdizioni europee sarebbero infatti competenti anche nel caso in cui un indiano o un cinese dovessero mai visitare un 'proprio' sito *web* durante le loro vacanze a Capri…

Più pragmaticamente, nell'Opinione del GEPD, ossia del Garante europeo per la protezione della *privacy*, Peter Hustinx, c'è da dire che questo approccio "non garantirà la piena protezione ai soggetti europei in una società disposta a rete, in cui le frontiere fisiche perdono importanza (…): l'informazione su internet è onnipresente, ma la giurisdizione del legislatore europeo non lo è"[26].

Tra le soluzioni prospettate dal GEPD per sopperire ai limiti di competenza delle autorità, non solo comunitarie, in materia di *privacy*, va annoverata l'elaborazione di un "quadro globale" per la protezione dei dati personali, sulla base delle linee guida elaborate dall'ONU e dall'OCSE; marco entro il quale sviluppare la cooperazione con altri organismi internazionali e con paesi terzi, anche in materia giurisdizionale, tramite accordi di stampo bilaterale o multilaterale.

Avendo, però, presente altri fattori rilevanti quali la corruzione e le istanze censorie di molti Paesi[27], nonché marcati contrasti politici tra le stesse istituzioni e Stati membri dell'UE[28], sembra proprio necessario integrare il "quadro globale" del GEPD con alcuni degli accorgimenti tecnologici discussi in questa sede.

Come detto, l'intento non è garantire un' "automatica applicazione della legge" in modo da prevenire del tutto la possibilità che si verifichi una qualsiasi trasgressione della *privacy*. Piuttosto, tramite il *design*, occorre attenuare il rischio che si verifichino eventi dannosi, consentendo agli individui di approntare da sé misure di sicurezza a tutela dei dati altrui o propri. È sotto questo punto di vista che può dunque scorgersi la possibile con-

[26] Si v. il par. 42 dell'Opinione del 25 luglio 2007 (EDPS, 2007/C 255/01).

[27] Cfr. solo R.J. DEIBERT, J.G. PALFREY, R. ROHOZINSKI, J. ZITTRAIN, *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, Mass., MIT Press, 2008.

[28] Tra i casi più significativi si pensi al regime del trattamento dati PNR, di cui mi sono ampiamente occupato in *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano, Giuffrè, 2008, pp. 157-196. Più di recente si v. E. BROUWER, *The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?*, CEPS Working Document n. 320, settembre 2009.

vergenza tra le tesi delle Autorità Garanti europee nel ricordato documento su "Il Futuro della Privacy" e le considerazioni del Commissario per la *privacy* in Ontario, secondo cui "dovesse mai crescere bene nel futuro, la privacy per design garantirebbe il futuro della privacy"[29].

Non si tratta, infatti, di rovesciare semplicemente le idee di chi, in nome dei ricavati tecnologici, si è peritato di annunciare nel corso degli ultimi anni la morte della *privacy*[30].

Si tratta al contrario di maturare la consapevolezza che molti dei problemi che affliggono l'odierna protezione dei dati personali s'intrecciano con le questioni coltivate ormai da tempo in altri campi, circa i profili di natura cognitiva, psicologica e tecnica del *design*[31].

Senza pretendere che gli accorgimenti tecnici del *design* ci indichino quale sarà mai il futuro della *privacy*, c'è da credere che proprio dal *design* avremo modo di comprendere molto sulla *privacy* del futuro.

[29] A. CAVOUKIAN, *Privacy by Design*, cit., p. 7.

[30] Tra i vari profeti mi limito a ricordare C. SYKES, *The End of Privacy. The Attack on Personal Rights at Home, at Work, On-Line, and in Court*, New York, St. Martin's Griffin, 1999; S. JARFINKEL, *Database Nation. The Death of Privacy in the 21st Century*, Sebastopol, O'Reilly, 2000; nonché D.H. HOLTZMAN, *Privacy Lost. How Technology Is Endangering Your Privacy*, San Francisco, Jossey-Bass, 2006.

[31] Si v. ad esempio D.A. NORMAN, *The Design of Future Things*, New York, Basic Books 2007; e S. KRUG, *Don't Make Me Think*, Indianapolis, New Riders, 2005.

Privacy e tutela dell'ordine pubblico in Europa e negli Stati Uniti: un differente approccio per raggiungere un difficile compromesso

GIUSEPPE VACIAGO*

SOMMARIO: *1. I dati digitali utili all'indagine – 2. Dati digitali pubblici e* social network *– 3. I dati digitali che identificano un soggetto e le operazioni che compie: gli indirizzi IP, i* log file *– 4. I contenuti digitali: le intercettazioni telematiche – 5. Conclusioni*

1. I DATI DIGITALI UTILI ALL'INDAGINE

I dati digitali che vengono generalmente richiesti in ambito investigativo possono generalmente dividersi fra quelli che consentono l'identificazione di un potenziale criminale (indirizzo IP), quelli che ne determinano l'attività *on line* (*log files*) e quelli che consentono di conoscere le sue conversazioni (intercettazioni telematiche).

Si ritiene, generalmente, che questo tipo di informazioni possa essere ottenuta solo attraverso una precisa richiesta da parte dell'autorità ai fornitori di connettività o ai *provider* che offrono servizi di posta elettronica e/o ospitano contenuti generati dagli utenti; tuttavia una gran parte di queste informazioni può essere anche indirettamente reperita semplicemente navigando in Rete.

Sono rimasto davvero sorpreso dell'efficacia del servizio offerto dalla società statunitense Intelius Inc. che fornisce, per un importo variabile da 1 a 10 dollari, le seguenti informazioni relative ad ogni cittadino americano: indirizzi in cui ha abitato, numero di telefono e di cellulare, indirizzo *e-mail*, precedenti penali, situazione economico-finanziaria e patrimoniale, precedenti attività lavorative e grado di scolarizzazione.

Tutte queste informazioni sono tratte, a detta della Società, da registri pubblici[1]: se questa affermazione, presente nel sito Intelius, fosse vera, dimostrerebbe che le informazioni pubbliche che ogni giorno vengono

* L'Autore è docente di Informatica giuridica alla Facoltà di Giurisprudenza dell'Università degli Studi dell'Insubria e avvocato del Foro di Milano.

[1] Curiosamente, tuttavia, la Società Intelius preferisce non chiarire nel dettaglio le modalità con cui vengono acquisiti tali dati (Articolo di Seattle News del 18 marzo 2009 presente al seguente indirizzo http://www.seattleweekly.com/2009-03-18/news/intelius-and-the-dubious-art-of-post-transaction-marketing/).

immesse in Rete, consentono di reperire un numero rilevante di dati finora ritenuti inaccessibili.

Attraverso un'accurata analisi di un profilo di Facebook o di un altro *social network*, è possibile recuperare dati utili non solo all'identificazione del soggetto, ma anche "intercettare" il contenuto di conversazioni potenzialmente utili ad un'indagine[2].

È evidente, pertanto, che i dati digitali devono anche essere classificati in funzione della loro accessibilità. Una simile distinzione diviene particolarmente rilevante in quanto, come vedremo, non è stata fino ad ora considerata adeguatamente soprattutto a livello europeo.

2. Dati digitali pubblici e *social network*

La Suprema Corte degli Stati Uniti ha sancito che "il quarto emendamento non proibisce di utilizzare informazioni rivelate da un soggetto ad una terza persona e da questa trasmesse all'Autorità governativa, anche se queste informazioni sono state rivelate nel presupposto di un utilizzo per uno scopo limitato"[3].

In Italia, l'attività di accertamento della polizia giudiziaria, che accede alle comunicazioni aperte a tutti i navigatori, per le quali non sia richiesto alcun codice di accesso, è liberamente utilizzabile: la giurisprudenza non ritiene che tale attività, infatti, costituisca "intercettazione delle comunicazioni private intercorse per via informatica o telematica di cui all'articolo 266 *bis* c.p.p. che, attenendo alla sfera personale, rientra nell'ambito della riservatezza costituzionalmente garantita"[4].

Questi principî, se applicati acriticamente alla realtà del *web 2.0*, consentono alle forze di polizia di accedere senza limitazioni, sia in fase inve-

[2] Tra i molti esempi che si possono citare, è sicuramente singolare l'arresto avvenuto in Italia di un latitante membro della "n'drangheta, scoperto, in quanto aveva aperto una pagina su facebook con lo pseudonimo di *scarface*" (articolo de La Stampa del 16 marzo 2010, presente al seguente indirizzo http://www.lastampa.it/redazione/cmsSezioni/cronache/201003 articoli/53173girata.asp).

[3] United States v. Miller, 425 U.S. 435, 443 (1976).

[4] Tribunale Milano, 30 ottobre 2002, in *Foro ambrosiano*, 2003, p. 55. La fattispecie era relativa alla consultazione di un sito relativo ad una vendita *on line* aperta ad un numero indeterminato di possibili clienti, del tutto assimilabile ad un'offerta di vendita di prodotti pubblicizzata su di una qualsiasi rivista cartacea di annunci commerciali.

stigativa, sia con finalità di prevenzione, a tutte le informazioni contenute all'interno dei *social network*.

Ne è conferma il recente progetto inglese denominato "Interception Modernisation Programme" che, sulla falsa riga del progetto statunitense "NSA Call Database", dovrebbe comportare la creazione di un *database* integrato in cui potrebbero venire memorizzati non solo i numeri di telefono chiamati e gli indirizzi *e-mail*, ma anche i siti *web* visitati di milioni di cittadini britannici.

Tale progetto, fortemente osteggiato dal gruppo a tutela della *privacy* APPG (*All Party Parliamentary Privacy Group*), ove dovesse diventare operativo, dimostrerebbe sicuramente la carenza di attenzione che, a livello europeo, fino ad ora è stata rivolta all'enorme potenziale delle informazioni contenute nel *web 2.0*.

Negli Stati Uniti, invece, la sensibilità al tema sembra essere maggiore, anche perché i servizi commerciali collegati ne evidenziano ancora di più i potenziali rischi[5].

"Date Check", uno dei servizi di Intelius, ad esempio, consente di conoscere tutte le informazioni sul proprio potenziale partner, semplicemente digitando dal proprio cellulare il suo numero di telefono: si passa dai dati personali, ai precedenti penali all'utilissimo stato di famiglia e, in pochi istanti, dal proprio cellulare si può sapere se la persona davanti a sé ha delle "intenzioni serie" o meno[6].

Oltre ai numerosi casi in cui le Università statunitensi e le forze di polizia hanno usato Facebook per investigare eventuali abusi di alcool, vi è un caso molto significativo che testimonia l'improprio utilizzo dei *social network* da parte delle forze di polizia[7]. Nel dicembre del 2006, la polizia del

[5] Per un approfondimento sul tema si veda T.P. CROCKER, *From Privacy To Liberty: The Fourth Amendment After Lawrence*, in "UCLA Law Review", n. 57, p. 1.

[6] Esemplificativo è il video che descrive le potenzialità del servizio: http://www.youtube.com/watch?v=WLc2JLYx78k&feature=player_embedded#; diverso, ma non per questo meno interessante, è il sito www.dondatehimgirl.com dove le ragazze deluse da un appuntamento, possono mettere in guardia le altre utenti del sito, descrivendo i comportamenti negativi del ragazzo con cui sono uscite.

[7] Articolo del Washington Post del 6 aprile 2009 di Michael Birnbaum disponibile al seguente indirizzo http://www.washingtonpost.com/wp-dyn/content/article/2009/4/05/AR2009040501880.html.

campus dell'Università del North Carolina, in un'indagine legata al furto di due *console* "playstation", aveva indirizzato i sospetti su due giovani che si trovavano nelle vicinanze del Cape Fear Community College. Avendo visto che uno dei due ragazzi aveva pubblicato su Facebook una propria foto con delle armi, decisero che era opportuno avvisare lo SWAT (*Special Weapons And Tactics*) per fare irruzione nell'abitazione degli studenti.

Il risultato dell'operazione fu tragico: uno degli agenti dello SWAT, scambiando il rumore della porta che veniva abbattuta per uno sparo, aprì il fuoco, causando la morte di uno dei ragazzi e del suo cane. Nessuna arma fu trovata all'interno dell'appartamento dei ragazzi.

Ovviamente questo è un esempio che non consente alcun tipo di generalizzazione, ma serve solo per ribadire l'esigenza di una seria riflessione sull'opportunità di considerare le informazioni ricavate dai *social networks* come meramente pubbliche.

Non dovrebbe sfuggire la differenza tra la pubblicazione di una pagina *web* e la pubblicazione di una foto all'interno di un *social network*. Nel primo caso è palese la mia intenzione di rendere pubblica una certa informazione, mentre nel secondo l'informazione che pubblico è destinata ad essere comunicata solo ad un particolare gruppo di amici.

Una interessante ricerca dell'Istituto "Privacy and Cybercrime" della Ryerson University a Toronto, ha dimostrato che un campione di 2000 studenti canadesi considera riservate le informazioni immesse in un *social network* (ossia che sia in vigore una sorta di "privacy del network") e non quelle pubblicate su siti *web*.

Lo stesso sondaggio mostra come le istituzioni scolastiche e il mondo dell'impresa non riconoscano tale "privacy del network", ed anzi utilizzino per i loro fini tali informazioni, in quanto reputano che, essendo immesse *on line*, esse siano pubbliche e non soggette ad alcuna protezione[8].

[8] Significativo un caso accaduto proprio in Canada dove una compagnia di assicurazioni ha cercato di negare il premio assicurativo ad una donna che soffriva di depressione, ma aveva inserito all'interno di facebook le foto di una vacanza dove sembrava divertirsi. La donna si è difesa sostenendo che aveva avvisato la compagnia assicurativa che sarebbe partita, in quanto il dottore le aveva consigliato come terapia una vacanza in un posto caldo. Il giudice ha deciso in favore della donna (articolo di CBC del 19 novembre 2009 disponibile al seguente indirizzo http://www.cbc.ca/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html).

In definitiva, la quantità e la qualità delle informazioni presenti *on line* potenzialmente utili ad un'indagine sono aumentate esponenzialmente e sono sempre più sfruttate dalle forze dell'ordine. Questa circostanza non dovrebbe essere sottovalutata e dovrebbe suscitare maggiore attenzione, almeno a livello giurisprudenziale, sul tipo di dati acquisibili durante la fase investigativa e successivamente utilizzabili in quella processuale: considerare il "domicilio virtuale" di un *social network* come un luogo liberamente accessibile significa non comprendere il ruolo e la finalità con cui tali strumenti vengono utilizzati.

È altrettanto vero che, come hanno spesso ricordato le Autorità Garanti della *privacy* in Europa, è importante che vi sia anche da parte delle nuove generazioni e non solo, una maggiore responsabilizzazione sul tipo di contenuti che all'interno di questo "domicilio virtuale" vengono immessi[9].

3. I DATI DIGITALI CHE IDENTIFICANO UN SOGGETTO E LE OPERAZIONI CHE COMPIE: GLI INDIRIZZI IP, I *LOG FILE*

L'indirizzo IP è un numero che identifica un dispositivo collegato a una rete telematica: esso può essere paragonato ad un indirizzo stradale o ad un numero telefonico. Il fornitore di connettività, infatti, dato un indirizzo IP e l'ora di accesso a tale indirizzo, è in grado di fornire i dati personali di chi ha sottoscritto il contratto per usufruire dei servizi di connessione. L'indirizzo IP, in sé, non offre nessuna informazione utile all'indagine, ma senza di esso non sarebbe possibile ottenere le corrette informazioni da parte del fornitore di connettività.

Il *file* di *log*, invece, è un file in cui vengono memorizzate le attività compiute da un determinato utente e consente, pertanto, di ricostruire la sua attività all'interno del *computer* o in Rete.

La conservazione di tali dati da parte dei *provider* di servizi *web* e dei fornitori di connettività (altresì definita *data retention*) consente di identificare con notevole precisione un utente della Rete e di conoscere quali tipi

[9] Gruppo "Articolo 29", *Parere 5/2009 sui Social Network On-Line*, disponibile *on-line* al seguente indirizzo http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_it .pdf.

di operazioni siano state da lui svolte. È chiara, pertanto, l'importanza di tali dati sotto un profilo investigativo.

Tuttavia, se l'indirizzo IP è un dato estremamente utile per un'investigazione digitale, lo stesso dato potrebbe essere anche utile a livello commerciale per la profilazione di un utente soprattutto se abbinato all'utilizzo dei *cookies*[10], come la recente direttiva sulla *privacy* nel settore delle comunicazioni elettroniche osserva[11].

Nel 2008 il Commissario europeo Peter Scharr, a capo del gruppo articolo 29 (gruppo composto dai Garanti europei per la *privacy*), ha sostenuto che l'indirizzo IP è un dato personale e pertanto deve essere soggetto alla tutela offerta dalla direttiva europea sulla *privacy*[12]. Questa dichiarazione ha aperto un dibattito con alcune società americane che hanno invece sostenuto che l'indirizzo IP è un dato che, da solo, non può consentire l'identificazione dell'utente e pertanto non necessita di una particolare tutela da parte della disciplina sulla *privacy*[13].

Non credo che questo dibattito meriti un approfondimento in questo articolo, ma ricordarlo è utile, per dimostrare come la *data retention* sia uno

[10] I *cookies* sono *file* di testo inviati da un *server* ad un *web client* e poi rimandati indietro dal *client* al *server* – senza subire modifiche – ogni volta che il *client* accede allo stesso *server*. I *cookies* sono usati per eseguire autenticazioni e memorizzare informazioni specifiche riguardanti gli utenti che accedono al *server*, come ad esempio i siti preferiti o, in caso di acquisti *on line*, il contenuto degli stessi.

[11] La direttiva europea 2009/136/CE del 25 novembre 2009 definitiva anche direttiva "e-privacy" oltre a rafforzare i poteri delle Autorità Garanti per la protezione dei dati personali in tutti gli Stati membri e introdurre nuove forme di tutela contro lo "spam" ha esplicitamente messo in guarda gli *Internet Service Providers* contro l'uso di alcuni *cookies* (c.d. *flash cookies*) che difficilmente possono essere rimossi da un computer (il testo della Direttiva è disponibile al seguente indirizzo http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri= OJ:L:2009:337:0011:0036:EN:PDF).

[12] Articolo della CBS del 21 gennaio 2008 disponibile al seguente indirizzo http://www.cbsnews.com/stories/2008/01/21/tech/main3734904.shtml?source=RSSattr =SciTech_3734904.

[13] Al seguente indirizzo *web* è disponibile la lettera di Peter Schaar alla società Google Inc.: http://epic.org/privacy/ftc/google/art29_0507.pdf e al seguente indirizzo è presente la risposta di Peter Fleischer, Global Privacy Counsel di Google Inc.: http://static.google usercontent.com/external_content/untrusted_dlcp/www.google.com/it/us/events/docs/ policyblog_peter_fleischer_statement.pdf.

dei casi dove risulta più palese la contrapposizione tra tutela della *privacy* e tutela dell'ordine pubblico.

È chiaro che, in questo caso, il fornitore di connettività si trova ad avere due "padroni": da un lato vi sono le pressioni dei Garanti della *privacy*, in Europa, e delle grandi associazioni a tutela della *privacy*, negli Stati Uniti, che si lamentano, come è successo nei confronti di Google, di una esagerata memorizzazione dei dati di identificazione. Dall'altro lato le Autorità giudiziarie chiedono, all'opposto, una più ampia e duratura memorizzazione dei dati.

In quale direzione è opportuno andare?

A livello europeo si è scelto di adottare una disciplina comunitaria molto dettagliata sulla *data retention* (direttiva 06/24/EC fortemente voluta proprio dall'Italia, che prevede all'articolo 5 un minimo di sei mesi fino ad un massimo di due anni di memorizzazione degli indirizzi IP e dei *file* di *log* di tutto il traffico *web*), ma il dibattito è tutt'altro che chiuso.

Negli Stati Uniti, infatti, anche se non è mancato chi ha ritenuto possibile una regolamentazione in tema di conservazione dei dati[14], sono state numerose e vibranti le proteste mosse sia da EPIC[15] (Electronic Privacy Information Center) che da EFF[16] (Electronic Frontier Foundation).

Ancora prima dell'emanazione della direttiva del 2006, inoltre, vi era chi sosteneva che una volta introdotto un obbligo di conservazione dei dati, il rischio maggiore sarebbe stato quello di un abuso di tali informazioni anche per scopi diversi da quelli per cui tale normativa era stata pensata, come ad esempio la richiesta di dati di connessione in caso di violazione di *copyright*[17].

[14] Da alcuni anni si discute infatti della possibilità di adottare una normativa specifica che preveda un determinato periodo di tempo di conservazione dei dati digitali. Va ricordato, inoltre, che il Sarbanes-Oxley Act del 2002 obbliga a conservare le mail della propria società per un periodo non inferiore a 5 anni.

[15] Si veda http://epic.org/privacy/intl/data_retention.html.

[16] Tra gli ultimi si veda l'articolo di E. KATZ, *The Beginning of the End of Data Retention Commentary*, disponibile al seguente indirizzo http://www.eff.org/deeplinks/2010/03/beginning-end-data-retention.

[17] J. ZITTRAIN, *Beware the Cyber Cops*, disponibile al seguente indirizzo http://www.forbes.com/forbes/2002/0708/062.html.

Le critiche non sono mancate anche in Europa: ne è una dimostrazione il fatto che ben 16 Stati membri su 27 abbiano espressamente richiesto una dilazione, in alcuni casi fino a 36 mesi, dall'emanazione della direttiva, per l'applicazione della stessa nel proprio Stato[18].

La Corte di Giustizia, inoltre, è dovuta intervenire nel marzo del 2009 rigettando il ricorso fatto dall'Irlanda e dalla Slovacchia che avevano chiesto l'annullamento della criticata direttiva[19].

La decisione della Corte di Giustizia della Comunità europea su tale ricorso non ha impedito un anno dopo alla Corte costituzionale tedesca di dichiarare l'incostituzionalità della legge sull'archiviazione di massa di dati telefonici e di navigazione su Internet, derivante dell'implementazione della direttiva. La Corte ha sostenuto che tale normativa viola la segretezza delle comunicazioni, archivia dati sensibili in mancanza di parametri di sicurezza per i cittadini ed è carente di informazioni precise in merito a come i dati verranno utilizzati[20].

Medesima decisione era stata raggiunta pochi mesi prima dalla Corte costituzionale romena[21].

Di questo scenario sono chiare le conseguenze da un punto di vista pratico: un ufficiale di polizia giudiziaria delegato ad un'indagine che veda coinvolto un *provider* di servizi statunitense, tedesco o rumeno, non potrà mai sapere se i dati che sta cercando sono già stati cancellati oppure sono ancora memorizzati e utilizzabili per le indagini.

[18] Significativo che tra questi Stati membri vi sia anche il Granducato di Lussemburgo, Stato in cui ha sede "Skype Europa".

[19] Il ricorso per l'annullamento della direttiva era fondato sul presupposto che la stessa fosse stata emanata non per armonizzare le legislazioni al fine di favorire il mercato interno nel settore delle comunicazioni elettroniche, bensì per favorire la raccolta di questi dati per scopi di sicurezza pubblica e lotta al terrorismo. Questi scopi, infatti, fanno parte della "cooperazione giudiziaria e di polizia in materia penale" e non dovrebbero essere regolati attraverso una direttiva comunitaria, secondo quanto sostenuto dai due Stati membri.

[20] Il video della decisione è presente al seguente indirizzo http://www.youtube.com/watch?v=7AU6cqG8nrI&feature=player_embedded.

[21] Decisione della Corte Costituzionale Romena n. 1258 dell'8 ottobre 2009 disponibile al seguente indirizzo http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-dataretention.html.

Il contrasto in questo caso è ancora più insanabile, in quanto l'autorità giudiziaria e la polizia investita delle indagini, non solo ritengono fondamentale la direttiva sulla *data retention*, ma ne vorrebbero un'applicazione anche per i gestori non europei che offrono servizi in Europa.

Pur comprendendo le difficoltà di chi deve quotidianamente combattere il crimine informatico e non solo, ritengo che raggiungere tale obiettivo sia estremamente complesso, in quanto casi come il *cyber-attacco* subito da Google in Cina (anche se mai ammesso dal Governo cinese) dimostrano chiaramente come le differenze politiche, sociali e culturali di ogni singolo Stato possano diventare una barriera invalicabile per società che operano a livello globale[22].

Tuttavia, la necessità di una soluzione a tali tematiche potrebbe non essere lontana, nel caso si riuscisse a dar seguito alle dichiarazioni programmatiche che si leggono nel documento congiunto redatto dall'Unione europea e dagli Stati Uniti dal titolo "Migliorare la cooperazione transoceanica nell'area della giustizia, libertà e sicurezza" adottato a Washington il 28 ottobre 2009: "Abbiamo significativi punti di contatti e un profondo e radicato impegno nella protezione dei dati personali, sebbene vi siano delle differenze nei nostri approcci", e poco dopo si legge "è nostra intenzione promuovere la modifica e l'implementazione della Convenzione sul Cybercrime del 2001[23].

Nello stesso senso il Consiglio d'Europa si è espresso nel documento: "Programma di Stoccolma. Un'aperta e sicura Europa in grado di proteggere i suoi cittadini" del 2 dicembre 2009[24].

[22] Nel gennaio del 2010 Google ha annunciato il suo ritiro dal mercato cinese dopo aver subito un pesante attacco da parte di alcuni *hackers*; pur non essendo esplicitato, si legge tra le righe di questo *post* pubblicato dalla società (http://googleblog.blogspot.com /2010/01/new-approach-to-china.html), che vi può essere un collegamento tra l'attacco subito e la decisione di Google di non fornire i dati di registrazione di alcuni utenti del suo servizio.

[23] Per una versione integrale del documento si veda il seguente indirizzo http://www.se2009.eu/polopoly_fs/1.21271.1256739594!menu/standard/file/EU-US%20Joint%20Statement%2028%20October%202009.pdf.

[24] Per una versione integrale del documento si veda il seguente indirizzo http://register.consilium.europa.eu/pdf/en/09/st14/st14449.en09.pdf.

4. I CONTENUTI DIGITALI: LE INTERCETTAZIONI TELEMATICHE

Se l'identificazione di un utente e l'analisi della sua attività *on line* destano così tanta preoccupazione sotto il profilo della protezione dei dati personali, è naturale che l'intercettazione dei contenuti delle conversazioni telematiche meriti una soglia di attenzione ancora più alta.

Le recenti statistiche dimostrano che, a livello europeo, l'Italia è il Paese che fa il più largo uso dell'intercettazione come mezzo di ricerca della prova nelle indagini[25]. Basti pensare che negli ultimi quattro anni il Ministero di giustizia italiano ha speso un 1,3 miliardi di euro per poter conseguire il seguente primato europeo: 1 cittadino ogni 500 abitanti è intercettato per un totale di quasi 150.000 richieste di intercettazioni all'anno.

Questi dati riguardano principalmente le intercettazioni telefoniche e non quelle telematiche, in quanto, in Italia, anche se ogni giorno vengono scambiate 464 milioni di e-mail, non sono ancora sufficientemente note le enormi potenzialità di questo tipo di intercettazione[26].

Una *e-mail*, a differenza di una telefonata, può essere immediatamente indicizzata con chiavi di ricerca determinate, contiene spesso allegati potenzialmente utili, e rende più facile la comprensione del contesto del discorso.

Se due commercianti di droga dovessero darsi via telefono un appuntamento in un determinato luogo ad una certa ora, come è possibile sapere se durante quell'incontro sarà consegnato un ingente quantitativo di droga oppure se i due andranno soltanto a bere un caffé per ricordare "i vecchi tempi"? Intercettando una email, invece, vi è la possibilità di raccogliere un numero maggiore di informazioni utili all'indagine anche perché, sempre più spesso, accade che un messaggio email contenga anche tutti i precedenti messaggi che gli utenti si sono scambiati tra loro.

Negli Stati Uniti, le statistiche relative alle intercettazioni sono molto diverse in quanto le richieste autorizzate di intercettazione all'anno sono

[25] J. LEYDEN, *Italy Tops Global Wiretap League*, disponibile al seguente indirizzo http://www.theregister.co.uk/2007/03/07/ wiretap_trends_ss8/; per un approfondimento sui costi delle intercettazioni in Italia si veda l'indirizzo http://punto-informatico.it/1860408/Telefonia/News/intercettazioni-governo-vuole-risparmiare.aspx.

[26] Fonte contactlab: http://www.contactlab.com/download/CONR09/CONR09_italy_extract_it.pdf.

1861 di cui 386 a livello federale e le restanti 1475 a livello statale[27]. Solo un cittadino su 165.000 abitanti è intercettato.

Da un punto di vista normativo, non essendovi una disciplina unitaria a livello europeo e considerando gli inquietanti primati italiani sul tema delle intercettazioni, è utile comparare la disciplina italiana a quella statunitense.

Se negli Stati Uniti manca una normativa che determini i limiti e i tempi di conservazione dei dati degli ISP e dei *providers*, certo non è così per quanto riguarda le intercettazioni telematiche che vengono regolate *dall'Electronic Privacy Communications Act* emanato nel 1986.

Con l'emanazione di questo atto, è stato chiarito che ogni intercettazione che non rispetti le condizioni previste dalla legge, deve essere considerata illegale e, oltre a comportare l'inutilizzabilità di tali informazioni all'interno del processo, può determinare un'azione di risarcimento del danno rivolta nei confronti del responsabile.

Questa normativa è divisa in tre titoli: il primo è dedicato specificamente alle intercettazioni delle comunicazioni telematiche (*Electronic Privacy Communications Act*, 18 U.S.C. § 2510), il secondo regola la possibilità di accedere ai contenuti memorizzati all'interno di un *computer* o di un *server* (*Stored Communications Act*, 18 U.S.C. § 2701) e il terzo riguarda la possibilità di monitorare gli accessi alla Rete da parte degli utenti, senza tuttavia poter conoscere il contenuto delle loro comunicazioni (*Pen Register Act*, 18 U.S.C. § 206).

Teoricamente, tra questi tre titoli, solo il primo riguarda specificamente le captazioni in tempo reale di informazioni digitali; tuttavia, ritengo opportuna una trattazione congiunta, in quanto, pur con le dovute distinzioni per quanto riguarda situazioni di urgenza, è molto sottile la differenza tra l'intercettazione di una e-mail attraverso un sistema di duplicazione della casella di posta elettronica e un accesso alla casella di posta elettronica nella forma prevista dallo *Store Communications Act*.

Sebbene in tutte e tre le ipotesi, il pubblico ministero debba ottenere un "warrant" (equivalente al nostro decreto) da parte del giudice competente (statale o federale in relazione al tipo di reato per cui si procede) prima che le forze di polizia o il *Federal Bureau of Invesigation* possano pro-

[27] Fonte U.S. Courts: http://www.uscourts.gov/wiretap08/Table2.pdf.

cedere, solo alla prima (intercettazione in senso proprio) quest'obbligo si applica rigidamente.

Infatti, nel caso delle informazioni memorizzate all'interno di un *computer* o di un *server* (*Stored Communication Act*), vi sono alcune specifiche eccezioni: nel caso in cui il *provider* si renda conto per circostanze casuali di un concreto e serio pericolo di vita per un soggetto, nel caso in cui debba tutelare i suoi diritti qualora fosse vittima di una frode[28] o nel caso in cui debba informare il *National Centre for Missing and Exploted Kids* per un'ipotesi di pedofilia *on line*.

Inoltre è possibile che le sole informazioni relative all'identità di un determinato utente (e non quindi i contenuti) possano essere ottenute anche attraverso un *subpoena* (diffida) che, tuttavia, non può essere fatta da un privato, ma deve comunque essere richiesta dall'autorità giudiziaria.

Nel caso del monitoraggio, invece, il *Pen Register Act* ha subìto sensibili modifiche con il *Patriot Act* e con l'introduzione della *National Security Letter* che hanno consentito una deroga notevole al principio generale.

La *National Security Letter* è una forma di *subpoena* di natura amministrativa, utilizzata dal *Federal Bureau of Investigation*, in forza della quale viene concessa a tale organo investigativo la possibilità di richiedere il monitoraggio di alcune informazioni (nome dell'utente, indirizzo, registro delle transazioni, intestazioni delle e-mail), senza sostanzialmente alcuna previa autorizzazione da parte del giudice[29].

In Italia, l'intercettazione viene disciplinata dal codice di procedura penale all'articolo 266-*bis*, mentre l'accesso ai dati digitali, contenuti in un *server* o in un *computer*, avviene attraverso il sequestro e non è prevista alcuna attività di monitoraggio preventivo sui dati[30].

Dal punto di vista procedurale la disciplina non si differenzia in modo significativo da quella statunitense. Infatti, il pubblico ministero chiede al giudice delle indagini preliminari (o al giudice nel corso del dibattimento

[28] *United States v. Harvey,* 540 F.2d 1345, 1350-52 (8th Cir. 1976).

[29] La *National Security Letter* dava anche la facoltà al FBI di segretare l'attività di monitoraggio fino alla dichiarazione di incostituzionalità avvenuta con il caso Ashcroft v. ACLU, 542 U.S. 656, 665-66 (2004).

[30] Disciplina che è stata recentemente riformata dalla legge 48/2008 di ratifica della Convenzione *Cybercrime* stipulata a Budapest il 23 novembre 2001.

o al giudice di pace in caso di reati di sua competenza) di emettere il decreto di autorizzazione allo svolgimento delle operazioni. Ove, invece, vi fossero ragioni di urgenza (art. 267 c.p.p.), sarebbe legittimo un provvedimento di autorizzazione del pubblico ministero: questi, tuttavia, deve tassativamente richiedere la convalida al giudice competente entro 24 ore dal suo provvedimento e il giudice deve autorizzare tale intercettazione entro 48 ore dalla richiesta.

Una volta autorizzato, il pubblico ministero dispone l'intercettazione con decreto, indicando modalità e tempi di esecuzione delle operazioni (massimo quindici giorni, che diventano quaranta in caso di intercettazioni preventive).

Proprio sui tempi di esecuzione si potrebbe porre un problema nell'applicazione dell'intercettazione telematica. Se, infatti, l'arco temporale in cui è ammissibile compiere delle intercettazioni è di 40 giorni, come si può considerare l'intercettazione di una e-mail che contiene al suo interno una precedente e-mail di due mesi prima?

Come già anticipato sopra, nella comunicazioni via e-mail si è soliti, attraverso il comando "rispondi" o "rispondi a tutti", mantenere la e-mail o tutte quelle precedenti. Se è indubbio che tale prassi favorisce gli investigatori, ne è meno certa la legittimità da un punto di vista procedurale.

Nella scarsa giurisprudenza sul tema delle intercettazioni telematiche un problema del genere non si è ancora posto, ma merita di non essere sottovalutato.

L'elenco dei reati in forza dei quali è possibile richiedere l'intercettazione telematica negli Stati Uniti è ampio (18 U.S.C. § 2516) e si divide tra:

- reati di competenza federale (tra cui a titolo meramente esemplificativo è possibile citare il sabotaggio delle centrali nucleari, reati collegati alle arme biologiche, lo spionaggio, la rivelazione di segreti industriali, la corruzione di un funzionario e le associazioni a delinquere finalizzate allo spaccio di stupefacenti);

- reati di competenza del singolo Stato (tra cui l'omicidio, il rapimento, il gioco d'azzardo, la rapina, la corruzione, l'estorsione, il traffico di stupefacenti, o altri crimini che possono cagionare danni fisici punibili con la reclusione superiore ad un anno).

In questo caso, la disciplina italiana è molto differente in quanto il codice di procedura penale (art. 266-*bis*), oltre a prevedere come presup-

posto per l'utilizzo dell'intercettazione una serie di reati ben definita (tra i più rilevanti possiamo citare i delitti per i quali è prevista la reclusione superiore nel massimo a cinque anni, i delitti contro la pubblica amministrazione e i delitti concernenti sostanze stupefacenti) ha anche previsto che siano compresi nell'elenco tutti i reati commessi mediante l'impiego di tecnologie informatiche o telematiche.

È molto probabile (se non quasi certo) che ogni reato che richieda un'intercettazione telematica, sia stato commesso anche "mediante l'impiego di tecnologie informatiche e telematiche": pertanto, anche se con riserve da parte della dottrina, si può affermare che in Italia non vi è una tassativa elencazione dei reati, ma sia possibile richiedere l'intercettazione per ogni singolo reato per cui vi è l'utilizzo di tecnologia informatica.

Un discorso a parte merita infine il *Foreign Intelligence Surveillance Act* del 1978 che definisce le procedure per la sorveglianza elettronica e la raccolta di informazioni, da agenzie nazionali od estere, relative a cittadini americani, al fine di proteggere gli Stati Uniti contro potenziali e attuali attacchi, sabotaggi o possibili atti terroristici.

Questo tipo di attività di sorveglianza può includere, oltre ai dati di registrazione di un utente, anche l'accesso ai contenuti delle sue comunicazioni: esso può avvenire senza un ordine del giudice, nel caso in cui sia richiesto dal Presidente degli Stati Uniti attraverso il Procuratore generale degli Stati Uniti; oppure attraverso un ordine della del *Foreign Intelligence Surveillance Court*, che dovrà valutare l'effettiva pertinenza (ossia se l'obiettivo della sorveglianza riguardi effettivamente una minaccia proveniente da uno Stato estero) e la legittimità di tale richiesta.

Da menzionare, infine, il CALEA (*Communications Assistance for Law Enforcement Act* - 47 U.S.C. § 1001-1021) che impone alle compagnie telefoniche di implementare la propria infrastruttura tecnologica per poter favorire eventuali attività di sorveglianza elettronica da parte delle forze dell'ordine.

In estrema sintesi, la vera differenza tra la disciplina italiana delle intercettazioni e quella americana non è tanto nella procedura, quanto nell'effettiva applicazione. Negli Stati Uniti vi è una massiccia applicazione dei sistemi di monitoraggio preventivo, mentre in Italia vi è, sicuramente, un abuso delle intercettazioni per ora solo telefoniche, ma che, molto probabilmente, diventeranno telematiche nei prossimi anni.

Nonostante vi sia questa tendenziale somiglianza, essa non basta per creare una forma di cooperazione più efficace degli accordi sulla mutua assistenza giudiziaria tra gli Stati Uniti d'America e l'Italia del 3 maggio 2006, che sostituiscono gli accordi del 1982, al fine di adeguarli al trattato sottoscritto dagli Stati Uniti con l'Unione europea il 25 giugno 2003.

Il tema è particolarmente delicato, in quanto i principali "detentori" delle informazioni digitali del mondo sono società come Google, Yahoo e Microsoft, che hanno sede negli Stati Uniti.

Per un Paese come l'Italia abituato ad intercettare con una frequenza paragonabile al consumo giornaliero di caffè, il dover affrontare un processo rogatoriale per ottenere tali informazioni è traumatico. Ogni giorno, mediamente, in Italia vengono autorizzate 464 intercettazioni, mentre negli Stati Uniti ne vengono autorizzate sei.

Sulla difficoltà di trovare una forma di cooperazione su questo tema, già il Consiglio d'Europa, nel 2001, in sede di ratifica della Convenzione *Cybercrime*, aveva evidenziato il problema, nella sua relazione illustrativa all'articolo 32, che copre la materia dell' "accesso transfontaliero ai contenuti memorizzati all'interno di un computer".

Il Consiglio affermava laconicamente che permettere ad un Stato membro della Convenzione di accedere ai dati contenuti in un *computer*, memorizzati da un utente o da una società di un altro Stato membro, è "questione particolarmente complessa che non è possibile affrontare in carenza di esperienze consolidate in materia"[31].

5. Conclusioni

Il mio lavoro sulle differenze tra l'Europa e gli Stati Uniti in relazione a due temi di grande attualità, come la tutela dei dati personali e l'ordine pubblico, richiede sicuramente approfondimenti e dibattito critico, ma consente di trarre tre prime conclusioni.

La prima è che non vi sono né vinti né vincitori, nel lungo dibattito relativo alla tutela dei dati personali dei cittadini di fronte alle esigenze

[31] Per un approfondimento sul tema, M. Gercke, *Understanding Cybercrime: A Guide For Developing Countries*, disponibile *on line* al seguente indirizzo http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide. pdf.

dell'ordine pubblico: se è criticabile la scelta dell'Europa di aver creato una politica sulla *data retention* senza aver chiaramente precisato per quali tipologie di reato tali dati dovessero essere forniti, lo è altrettanto lo scandalo scoppiato durante l'amministrazione Bush circa l'accordo segreto della *National Security Agency* con i principali gestori di telefonia statunitensi, finalizzato a creare un database di tutte le telefonate e le attività *on line* compiute dai cittadini americani (con tutte le ovvie attenuanti che si riassumono nella data dell'11 settembre).

Alla stessa stregua se il numero delle intercettazioni a livello italiano è decisamente sproporzionato rispetto alla dimensione del Paese, non va dimenticato che le statistiche sul numero delle intercettazioni negli Stati Uniti non riguardano le richieste che vengono effettuate in forza dal FISA (*Foreign Intelligence Surveillance Act*).

La seconda considerazione è che il documento programmatico redatto a Washington il 28 ottobre del 2009 tra Unione europea e Stati Uniti e le affermazioni contenute nel programma di Stoccolma del 2 dicembre 2009 del Consiglio di Europa, sono e devono essere due importanti stimoli per l'effettiva implementazione della convenzione *Cybercrime* che, alla luce dell'esperienza acquisita dal 2001 ad oggi, permetta di trovare un punto di incontro tra la regolamentazione europea e quella statunitense.

La terza e ultima considerazione è un auspicio: le enormi potenzialità di Internet non possono soltanto essere utilizzate per incontrare i vecchi amici del liceo o per videotelefonare gratuitamente ai propri cari. Proprio la capacità di Internet di interconnettere a livello globale le persone e di essere potenzialmente uno strumento universale di pace deve essere il punto di partenza per la creazione di un sistema di regole a tutela della *privacy* e a tutela dell'ordine pubblico che siano valide per tutti. Prima dell'avvento di Internet siamo riusciti a stilare la Dichiarazione universale dei diritti umani.

Cosa potremmo fare con Internet?

L'Internet di seconda generazione e il diritto

Riflessioni sul diritto d'accesso a Internet nell'ambito del diritto dell'Unione europea

FRANCESCA BADOCCO*

SOMMARIO: *1. La società dell'informazione e Internet – 2. Il ruolo della Commissione europea nel quadro delle politiche per la promozione della società dell'informazione e dell'accessibilità al* web *– 3. L'atteggiarsi delle altre istituzioni rispetto a Internet e al diritto d'accesso – 4. L'attuale quadro giuridico di riferimento in materia di telecomunicazioni – 5. Osservazioni conclusive*

1. LA SOCIETÀ DELL'INFORMAZIONE E INTERNET

Sul finire degli anni Novanta si forma la consapevolezza, tradotta negli atti delle istituzioni, che il passaggio a un'economia digitale basata sulla conoscenza rappresenta un considerevole fattore di crescita e di competitività, determinando un miglioramento della qualità di vita dei cittadini. In tale contesto, è avvertita l'esigenza di concorrere alla formazione progressiva di una società dell'informazione aperta a tutti.

In Europa, lo sviluppo del concetto di società dell'informazione e dei suoi riflessi pratici ha radici lontane e affonda la sua ragion d'essere sicuramente in esigenze di carattere economico. Si può senza dubbio affermare che la rivoluzione delle comunicazioni è alimentata dalle tecnologie e dalle forze del mercato. È noto che servizi di telecomunicazione di elevata qualità favoriscono l'efficienza e la competitività del settore terziario e di tutti i comparti industriali. L'utilizzazione diffusa degli strumenti per lo scambio e il trattamento di transazioni, i documenti digitali, lo sviluppo delle reti aperte, costituiscono il modo per migliorare la qualità della vita dei cittadini, unitamente alla competitività del sistema economico. Con il mutare delle circostanze, gli elementi caratterizzanti la società dell'informazione si traducono nella necessità di sostenere le iniziative volte a promuovere i singoli aspetti della medesima, soprattutto a vantaggio della vita degli individui, attraverso la loro attiva partecipazione.

* L'Autrice è avvocato specializzato in Diritto della proprietà industriale e Diritto dell'Unione europea.

Dal punto di vista giuridico, rilevano gli articoli 170 e seguenti TFUE[1], i quali fungono da base per l'adozione di strumenti a supporto della società dell'informazione. In materia, é previsto che "l'Unione concorre alla costituzione e sviluppo di reti transeuropee nei settori delle…telecomunicazioni…". È di tutta evidenza come si tratti di un settore in cui è richiesta una piena collaborazione degli Stati membri per la realizzazione degli obiettivi della società dell'informazione. In altre parole, la materia delle telecomunicazioni, nelle sue differenti applicazioni in particolare per quanto riguarda il diritto di accesso a Internet, richiede lo sforzo congiunto degli Stati membri e delle istituzioni dell'Unione europea. Questo elemento appare particolarmente importante oggi, a seguito del tentativo di razionalizzazione normativo effettuato da Parlamento e Consiglio attraverso l'approvazione del "pacchetto telecom"[2].

Ora, anche alla luce delle recenti modifiche al quadro giuridico di riferimento, nasce quindi l'esigenza di comprendere se nel quadro della società dell'informazione così come delineatasi – e in via di progressiva, costante evoluzione – sia possibile riconoscere a tale diritto un'autonomia concettuale pari a quella che sta assumendo a livello internazionale. E, in caso affermativo, se sia possibile riconoscere al diritto in questione anche autonomia fattuale. In altre parole, si tenterà di dimostrare che v'è margine per ritenere che il diritto d'accesso a Internet nell'ambito dell'Unione europea possa valere, anche nella sua estrinsecazione concreta, quanto i diritti fondamentali di cui permette l'espressione.

1. Il ruolo della Commissione europea nel quadro delle politiche per la promozione della società dell'informazione e dell'accessibilità al *web*

Per verificare la tesi proposta, è opportuno analizzare le azioni concrete poste in essere nel settore delle tecnologie dell'informazione e della

[1] Trattato sul funzionamento dell'Unione europea, già Trattato della Comunità europea, così come modificato e rinominato, conformemente al Trattato di Lisbona, firmato il 13 dicembre 2007 (GUUE C 306 del 17 dicembre 2007) ed entrato in vigore il 1° dicembre 2009.

[2] In seguito all'entrata in vigore delle direttive 2009/136/CE e 2009/140/CE, facenti parte del "pacchetto telecom", gli Stati membri hanno termine fino al 25 maggio 2011 per adottare e pubblicare le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla direttive medesime.

comunicazione. In materia, emerge il ruolo centrale svolto dalla Commissione europea come soggetto sia promotore sia attuatore. Essa, in particolare attraverso la Direzione Generale società dell'informazione (e media), si occupa di elaborare piani e iniziative per la promozione dell'adozione delle tecnologie dell'informazione e della comunicazione, interessandosi anche ai rapporti tra gli operatori del settore, sia nelle attività produttive sia in quelle di erogazione dei servizi pubblici e privati. Tale compito si è andato intensificando dal 1998, a seguito della liberalizzazione del mercato europeo delle telecomunicazioni[3].

L'opera di armonizzazione del quadro regolamentare delle telecomunicazioni e delle comunicazioni mobili ha inevitabilmente aperto nuovi scenari nell'ambito dell'Unione europea. Tali politiche dimostrano la volontà delle istituzioni – della Commissione europea, in particolare – di rafforzare un approccio comune in materia di *e*-accessibilità e di accessibilità al *web*, essendo peraltro anche rivolte a favorire l'accesso delle persone disabili e degli anziani. Funzionale al raggiungimento di tale obiettivo è la prevenzione del "divario digitale", partita che si gioca su più fronti: da una parte, tra le regioni più ricche e quelle più povere (spesso periferiche), con minori possibilità di accesso a Internet; dall'altra, tra i diversi Stati membri dell'Unione europea.

Nell'ambito dei provvedimenti adottati in materia dalla Commissione europea per l'attuazione di specifiche politiche, si segnala la Comunicazione dell'8 dicembre 1999, relativa a un'iniziativa della Commissione europea in occasione del Consiglio europeo di Lisbona del 23 e 24 marzo 2000[4]. Il provvedimento in esame ha avuto il pregio di individuare già allora, nel dettaglio, le reali esigenze sottese alla promozione della società dell'informazione, tra le quali anche la necessità di incoraggiare l'accesso ad Internet.

Concentrando l'attenzione sugli strumenti che hanno inciso su tale diritto, appare innanzitutto considerevole l'impegno istituzionale della Commissione europea per la diffusione dell'accesso alla banda larga[5].

[3] Direttiva 96/19/CE della Commissione europea, del 13 marzo 1996, che modifica la direttiva 90/388/CEE al fine della completa apertura alla concorrenza dei mercati delle telecomunicazioni, in GUCE L 074 del 23 marzo 1996.

[4] Comunicazione COM(1999) 687 sull'iniziativa eEurope - Una società dell'informazione per tutti.

[5] Comunicazione COM(2006) 129 del 20 marzo 2006 per colmare il divario sulla banda larga.

Tale obiettivo si fonda sulla considerazione che il rapido accesso a Internet è essenziale per stimolare una società dell'informazione in Europa, con tutte le implicazioni a esso associate. È stato rilevato che la mancanza di una connessione ad Internet, che permette quindi l'accesso al *web*, colpisce in particolare le regioni tecnologicamente meno avanzate con ripercussioni immediate in termini di divario digitale, richiedendo quindi un'azione tempestiva[6]. Per far fronte a questa esigenza, attraverso lo strumento di cui sopra, la Commissione europea ha promosso una divisione del territorio europeo in aree di accesso ad Internet, identificando un numero di strumenti da sviluppare al fine di migliorare la disponibilità di connessione a banda larga.

A tale proposito, è rilevante la raccomandazione della Commissione europea sull'alfabetizzazione mediatica nell'ambiente digitale, per una società della conoscenza inclusiva[7]. Tale raccomandazione è successiva a una precedente comunicazione della Commissione europea del dicembre 2007, volta a promuovere un approccio europeo alla alfabetizzazione mediatica nell'ambiente digitale, sebbene sostanzialmente relativa alla comunicazione commerciale, agli audiovisivi, ai contenuti digitali.

Alla luce della formulazione della recente raccomandazione, è evidente che il raggiungimento degli obiettivi nell'ambito della alfabetizzazione digitale costituisce una tappa fondamentale nel processo di affermazione, o meglio rafforzamento, come diritto umano del diritto d'accesso a Internet. D'altro canto, la questione dell'e-accessibilità e dell'accessibilità del *web* ha acquisito maggiore visibilità politica negli ultimi anni, in particolare in seguito alla dichiarazione di Riga del 2006[8].

[6] Interessante segnalare che la Commissione europea, in data 8 febbraio 2010, ha approvato un regime di aiuto di stato per colmare il divario digitale della regione Lombardia – Decisione n. 596/2009, consultabile sul sito http://ec.europa.eu/competition/state_aid/register/.

[7] Raccomandazione 2009/625/CE. del 20 agosto 2009 sull'alfabetizzazione mediatica nell'ambiente digitale per un'industria audiovisiva e dei contenuti più competitiva e per una società della conoscenza inclusiva.

[8] La dichiarazione è il frutto dei lavori svolti in seno alla Conferenza Ministeriale Tecnologie dell'Informazione e della Comunicazione per una società inclusiva svoltasi nei giorni 11-12 e 13 giugno 2006 a Riga. Essa ha il pregio di riaffermare concetti fondamentali quali, tra gli altri, il fatto che le tecnologie dell'informazione e della comunicazione rappresentano un fattore di crescita del prodotto interno lordo e della produttività e contribuiscono

È chiaro l'interesse dell'Unione europea che tutti gli Stati membri migliorino l'accessibilità al *web*, conformemente agli impegni presi nella menzionata dichiarazione ministeriale. In questo quadro, come detto, la Commissione europea svolge un ruolo di sostegno per gli sforzi intrapresi dagli Stati membri. Tutto ciò è quindi finalizzato alla formazione di un approccio comune in tali settori, al fine di rendere la società dell'informazione accessibile a tutti i cittadini dell'Unione europea.

3. L'atteggiarsi delle altre istituzioni rispetto a Internet e al diritto d'accesso

S'è visto come la Commissione europea dia l'impulso e segua l'evolversi della società dell'informazione, in conformità ai compiti istituzionali attribuitili. Tuttavia, anche le altre istituzioni sono coinvolte a pieno titolo nel processo di sviluppo della medesima società dell'informazione per quanto riguarda l'accessibilità a Internet.

In questo quadro, si segnala la risoluzione del Parlamento europeo del 6 luglio 2006, frutto del dibattito sulle restrizioni ai contenuti di Internet e alla libertà di espressione delle persone che utilizzano tale mezzo di comunicazione[9]. Attraverso questo strumento il Parlamento europeo ha riaffermato, anche sulla base delle discussioni nell'ambito dal Vertice Mondiale sulla Società dell'Informazione (2003-2005)[10], che "l'accesso ad Internet può rafforzare la democrazia e contribuire allo sviluppo econo-

a migliorare la qualità della vita e la partecipazione sociale; che le persone anziane o con bassa scolarizzazione e i disoccupati utilizzano Internet in percentuale nettamente ridotta rispetto al resto della popolazione; che occorre dimezzare la differenza percentuale che esiste nell'uso di Internet tra gli utenti medi e le categorie deboli o svantaggiate; che le politiche di *e-inclusion*, pur implicando l'"inclusività" delle tecnologie dell'informazione e della comunicazione, richiedono soprattutto che l'utilizzo delle stesse sia finalizzato per ottenere una maggiore inclusione.

[9] Risoluzione del Parlamento europeo del 6 luglio 2006 sulla libertà di espressione su Internet (P6_TA(2006)0324).

[10] Tale vertice, promosso attraverso la Risoluzione 56/183 dell'Assemblea Generale delle Nazioni Unite del 21 dicembre 2001, si è svolto in due fasi, una prima a Ginevra nel dicembre 2003, una seconda a Tunisi a novembre 2005. Oggi, la continuità nei lavori è assicurata sul piano della implementazione della medesima a livello internazionale con regolari incontri delle parti coinvolte.

mico e sociale di un paese e che limitare tale accesso è incompatibile con il diritto alla libertà d'espressione"[11]. Essa ha il pregio di mostrare l'atteggiamento di apertura del (di una parte del) Parlamento europeo in materia di accesso ad Internet e del diritto di espressione, "considerando che l'Unione europea dovrebbe dimostrare che i diritti degli utenti di Internet sono al centro delle sue preoccupazioni".

Nella stessa sede, è recentemente stato elaborato un altro importantissimo documento sull'importanza dell'accesso ad Internet come diritto fondamentale del cittadino digitale. Si tratta della raccomandazione Lambridinis[12], avente ad oggetto il rafforzamento della sicurezza e delle libertà fondamentali su Internet, adottata peraltro pochi mesi prima della discussione definitiva delle modifiche da apportare ai provvedimenti normativi disciplinanti il settore delle telecomunicazioni.

La raccomandazione si segnala per la portata innovativa, manifestando una controtendenza nell'ambito dell'Unione europea rispetto a leggi avanzate in Francia e in altri Stati membri, contemplanti sanzioni automatiche in caso di violazione, per esempio, di diritto d'autore attraverso la condivisione *on-line* di *files* protetti. La raccomandazione afferma il principio secondo cui gli Stati, nonché gli operatori preposti, compagnie telefoniche e *service providers*, non possono impedire al titolare di una connessione Internet di non utilizzarla[13]. In particolare, gli Stati membri sono espressamente chiamati a "evitare tutte le misure legislative o amministrative che possono avere un effetto dissuasivo su ogni aspetto della libertà di espressione". Ciò sulla base, innanzitutto, della considerazione che Internet "dà pieno significato alla definizione di libertà di espressione" e che "può rappresentare una straordinaria possibilità per rafforzare la cittadinanza attiva".

[11] Punto D. della Risoluzione.

[12] Raccomandazione del Parlamento europeo al Consiglio del 26 marzo 2009 sul rafforzamento della sicurezza e delle libertà fondamentali su Internet (P6_TA(2009)0194).

[13] Principio non integralmente recepito nelle modificazioni del quadro normativo sulle telecomunicazioni preesistente ma temperato dalla possibilità di disconnettere il titolare in determinati casi. Per questa ragione, il "pacchetto telecom" è stato un compromesso, di cui si sarebbe potuto fare a meno.

4. L'attuale quadro giuridico di riferimento in materia di telecomunicazioni

Le indicazioni circa le politiche, l'atteggiarsi delle istituzioni e i benefici di carattere economico, e oggi anche sociale, determinati dall'implementazione della società dell'informazione aiutano a comprendere le ragioni per cui sia stato necessario rivedere la normativa che disciplinava il settore delle telecomunicazioni, risalente al 2002.

Tali esigenze già emergono nella comunicazione del 29 giugno 2006, con la quale la Commissione incoraggiava una revisione della legislazione in materia di telecomunicazioni[14]. In particolare, si auspicava una revisione degli strumenti giuridici in vigore sulla base della considerazione che il quadro normativo vigente, pur avendo prodotto vantaggi notevoli, dovesse tenere in considerazione le nuove esigenze, anche sociali, per essere efficace nel decennio successivo.

Proprio su questo punto, sempre la Commissione europea, ha avviato una consultazione nel settembre 2009, sollecitando l'intervento della società civile. In particolare, è stato dato rilievo alla determinazione dei diritti e, fra questi il riconoscimento esplicito del diritto d'accesso a Internet, qualificato come fondamentale, alla sua estensione e a taluni aspetti, quali la portabilità dei servizi e l'accesso a tutti dei medesimi. In questo contesto, si è giunta alla elaborazione di una revisione globale delle norme in materia di telecomunicazioni, volta, nel suo complesso, a rafforzare i diritti degli utenti di Internet e a incoraggiare la concorrenza nell'ambito delle comunicazioni elettroniche, nonché a promuovere gli investimenti nelle reti di nuova generazione.

La revisione normativa citata comprende tre provvedimenti, adottati nell'ambito della procedura di codecisione, i quali compongono quindi il "pacchetto telecom"[15].

Innanzitutto, il Parlamento europeo e il Consiglio hanno istituito l'Organismo dei regolatori europei delle comunicazioni elettroniche

[14] COM(2006) 334 sul riesame del quadro normativo comunitario per le reti ed i servizi di comunicazione elettronica.

[15] Si tratta del regolamento (CE) 1211/2009, della direttiva 2009/136/CE e della direttiva 2009/140/CE, pubblicati su GUUE L 337 del 18 dicembre 2009.

(BEREC) e l'Ufficio del medesimo, utilizzando lo strumento regolamentare[16]. Tale organismo, che assorbe le competenze di un precedente organismo regolatore e contempla maggiori poteri di coordinamento, ha sostanzialmente il compito di promuovere la cooperazione tra le autorità regolamentari nazionali e tra queste ultime e la Commissione europea. Esso inoltre riveste funzioni di consulenza per quest'ultima, nonché per il Parlamento europeo e il Consiglio. Come si intuisce, questo elemento enfatizza la necessaria cooperazione degli Stati membri, anche a livello amministrativo, per garantire, l'uniforme miglioramento nell'ambito dell'Unione europea delle condizioni d'accesso ai servizi telematici.

Accanto a tale regolamento, sono state approvate due direttive che incidono sul cuore normativo delle telecomunicazioni, a sua volta costituito da numerose precedenti atti aventi la medesima forma giuridica.

La materia è pertanto regolata dalla direttiva 2009/136/CE (diritti dei cittadini), recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e dal regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori[17]. Infine, è stata elaborata la direttiva 2009/140/CE (migliore regolamentazione), recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica[18].

Per quel che qui interessa, tralasciando gli innumerevoli interessanti spunti di riflessione e di comparazione tra la normativa attuale e quella preesistente e concentrandosi piuttosto sul diritto d'accesso a Internet, l'attenzione deve essere rivolta alla direttiva 2009/140/CE.

[16] Regolamento (CE) 1211/2009 del 25 novembre 2009.

[17] Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009.

[18] Direttiva 2009/140/CE del Parlamento europeo e del Consiglio del 25 novembre 2009.

Innanzitutto, si segnala come i "considerando" di questa direttiva assumano particolare rilevanza, laddove rappresentano, a parere di chi scrive, l'evoluzione della percezione dell'importanza assunta da Internet, anche quale strumento per l'esercizio dei diritti fondamentali[19]. I principî ivi contenuti, che informano tutte le modifiche intervenute sulla direttiva in discussione, presentando peraltro una matrice comune con quelli posti a fondamento degli altri due atti normativi che costituiscono il "pacchetto telecom", riconoscono che "Internet è essenziale per l'istruzione e l'esercizio pratico della libertà di espressione e l'accesso all'informazione" e che pertanto "qualsiasi restrizione imposta all'esercizio di tali diritti fondamentali dovrebbe essere conforme alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali". In secondo luogo, appaiono di sicuro interesse le disposizioni inserite sia nell'art. 1 della direttiva 2009/140/CE, che incide sulla direttiva 2002/21/CE – direttiva quadro –, sia nell'art. 2 della direttiva 2009/140/CE, recante modificazioni della direttiva 2002/19/CE, su aspetti tecnici del diritto d'accesso – direttiva accesso –[20].

La novità più rilevante consiste sicuramente nella previsione, contenuta nella direttiva quadro, secondo la quale "I provvedimenti adottati dagli Stati membri riguardanti l'accesso o l'uso di servizi e applicazioni attraverso reti di comunicazioni elettroniche, da parte degli utenti finali, devono rispettare i diritti e le libertà fondamentali delle persone fisiche, garantiti dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principî generali del diritto comunitario".

Peraltro "qualunque provvedimento di questo tipo riguardante l'accesso o l'uso dei servizi e applicazioni attraverso reti di comunicazione elettronica, da parte degli utenti finali, che ostacolasse tali diritti o libertà fondamentali può essere imposto soltanto se appropriato, proporzionato e necessario nel contesto di una società democratica e la sua attuazione deve essere oggetto di adeguate garanzie procedurali conformemente alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle liber-

[19] Al proposito, si veda il considerando n. 4 della direttiva 2009/140/CE.

[20] Si ritiene che tale tecnica legislativa trovi la sua ragion d'essere nelle circostanze che hanno portato all'elaborazione delle modifiche e rifletta la necessità di enucleare a livello di principio le garanzie sull'accesso ad Internet.

tà fondamentali e ai principî generali del diritto comunitario, inclusi un'efficace tutela giurisdizionale e un giusto processo. Tali provvedimenti possono di conseguenza essere adottati nel rispetto del principio della presunzione d'innocenza e del diritto alla privacy".

In altre parole, qualunque provvedimento che restringa l'accesso a Internet potrà essere imposto solo se ritenuto "appropriato, proporzionato e necessario nel contesto di una società democratica". E a condizione che, "nel rispetto del principio della presunzione d'innocenza e del diritto alla privacy", sia garantita "una procedura preliminare equa e imparziale, compresi il diritto della persona o delle persone interessate di essere ascoltate". Deve essere inoltre garantito "il diritto a un controllo giurisdizionale efficace e tempestivo".

Ora, l'inserimento di queste previsioni – in particolare, nella direttiva quadro – rappresenta una conquista d'indubbio rilievo. In questo modo si riconosce al diritto d'accesso a Internet una protezione giuridica equivalente a quella garantita a un diritto o a una libertà fondamentale[21].

Quanto agli aspetti più tecnici, cioè alla possibilità e all'adeguatezza dell'accesso, alla interconnessione e interoperabilità dei servizi, alle garanzie di trasparenza, si fa invece riferimento alla direttiva 2002/19/CE – direttiva accesso –. Le modifiche apportate in tale ambito sono confluite nell'art. 2 della direttiva 2009/140/CE e, come anticipato, riguardano sostanzialmente caratteristiche tecniche dei servizi Internet, riconoscendo importanti competenze in capo alle autorità di regolamentazione nazionali, coordinate dal nuovo organismo istituito a questo fine a livello europeo.

5. Osservazioni conclusive

In base alla nuova normativa, dalle azioni appena descritte, se si vuole, anche dalle dichiarazioni d'intenti delle istituzioni, soprattutto della Commissione europea, dovrebbe essere possibile tentare di rispondere al quesito posto all'inizio.

Più in particolare, nell'ambito dell'Unione europea, si tratta di prendere atto del quadro delle dichiarazioni, delle azioni concrete intraprese,

[21] Così si è espresso anche il Parlamento europeo, che ha fortemente voluto l'inserimento di questo nuovo paragrafo nella direttiva attualmente in vigore.

nonché delle novità giuridiche introdotte a seguito dell'approvazione del "pacchetto telecom".

Analizzando gli atti giuridici e non, illustrati in precedenza, attraverso i quali l'Unione europea ha collocato fra le priorità, al pari della Comunità internazionale, la necessità di colmare il divario digitale, di promuovere l'alfabetizzazione mediatica e, da ultimo, di razionalizzare tutte queste politiche attraverso lo strumento dell'Agenda digitale, è possibile concludere ipotizzando che il diritto d'accesso ad Internet nell'ambito dell'Unione europea rivesta una portata più ampia rispetto a quella riconosciutagli sul piano internazionale. Tale diritto non godrebbe, infatti, semplicemente di autonomia logico-giuridica, con ciò ritenendolo "affrancato" rispetto a uno dei diritti fondamentali più prossimi – la libertà d'espressione –. Dalla analisi effettuata, sembrerebbe infatti possibile attribuire al medesimo una sorta di autonomia in concreto, cioè nella sua dimensione fattuale.

Così ragionando si potrebbe ammettere un'autonomia a tutto tondo del diritto in questione, in definitiva sganciata da qualsiasi pregiudizio effettivamente sofferto sotto il profilo della limitazione dell'esercizio degli altri diritti fondamentali dei quali permette l'estrinsecazione.

Se questa ricostruzione è fondata – come pare dall'analisi dei documenti e della concreta attuazione dei principî in essi promossi e sanciti – tale diritto potrebbe essere utilizzato come parametro di giudizio alla stregua degli altri diritti fondamentali, a beneficio di tutti i soggetti legittimati ad azionarli.

La disciplina giuridica della seconda vita in Internet: l'esperienza *Second Life*

ELENA BASSOLI*

1. INTRODUZIONE A *SECOND LIFE*

Internet è, come noto, per sua natura, delocalizzato, a-territoriale e privo di uno spazio e un tempo ben definiti[1]. Esso, infatti, lungi dall'identificarsi con le macchine che lo compongono, è sincronicamente ovunque e in nessun luogo, così da costituire un mondo parallelo al mondo reale. In una evoluzione ormai prossima non è difficile prevedere una trasformazione, anche psicologica, degli utenti della Rete, che si muoveranno all'interno di essa per mezzo di propri *Avatar*[2], dotati di sembianze umane, ma privi di corporeità, come già accade in *Second Life*.

Del fenomeno *Second Life* in Internet si cominciò a discutere nel 2003, allorquando questo mondo virtuale tridimensionale venne creato dalla

* L'Autrice, avvocato in Genova, esperta di nuove tecnologie, è docente di Diritto dell'Informatica alla Facoltà di Giurisprudenza dell'Università degli Studi di Genova, della Statale di Milano e dell'Università del Piemonte Orientale. Autrice di oltre 120 pubblicazioni in materia e del *software* Verslex, in uso presso il Senato della Repubblica per l'aiuto alla redazione dei testi normativi, è Presidente di CSIG-Genova (Centro Studi Informatica Giuridica) e dottore di ricerca in "Metodi e tecniche della formazione e della valutazione delle leggi".

[1] Sulla caratteristica di non-luogo di *Internet* cfr. N. IRTI, *Norme e luoghi,* Laterza, 2006.

[2] Su Wikipedia si trova una calzante definizione del termine "Avatar": per Avatar deve intendersi un'immagine scelta per rappresentare la propria utenza in *community*, luoghi di aggregazione, discussione, o di gioco on-line. La parola, che è in lingua sanscrita, è originaria della tradizione induista, nella quale ha il significato di incarnazione, di assunzione di un corpo fisico da parte di un dio: per traslazione metaforica, nel gergo di internet si intende che una persona reale che scelga di mostrarsi agli altri, lo faccia attraverso una propria rappresentazione, un'incarnazione: un Avatar appunto.

società californiana *Linden Labs*. Tecnicamente dovrebbe parlarsi di videogioco di ruolo di massa (MMORPG)[3], ma la sua diffusione ne fa ormai un fenomeno sociale a livello planetario.

L'idea di ambientare una seconda vita sulla Rete delle reti non è nuova, essa ha interessato e appassionato scrittori di ogni genere e anche la filmografia ha spesso fatto ricorso a tale espediente per raccontare i paradossi delle vite virtuali, così dissimili da quelle reali, ma così intensamente vissute da non riuscire a discernere più la realtà dalla finzione, lasciando spesso al lettore il dubbio che quella vissuta da noi ogni giorno non sia la vera realtà.

Ad oggi i tempi appaiono maturi per arrivare a immaginare un mondo sempre più interconnesso e interoperabile, ove il virtuale è più reale del reale. Basti pensare alla gestione dei nostri risparmi affidati ormai alla moneta virtuale, sicché, se tutti i risparmiatori ritirassero contemporaneamente la cartamoneta equivalente a quanto risultante dall'estratto conto virtuale, non un solo istituto di credito resisterebbe.

Oppure ai nostri dati detenuti negli uffici dell'anagrafe. Se il sistema informatico comunale andasse in crash, sarebbe la fine delle identità.

Second Life è un gioco *on-line* con la diversità di non avere ambientazioni e missioni specifiche; la novità del gioco è la completa destrutturazione, consente a chiunque di fare pressoché qualsiasi cosa.

Così SL, proprio per la sua connotazione generalista e aspecifica, al pari della vita reale, ben si presta a rappresentare una formidabile palestra giuridica per il futuro, quando le nostre vite saranno, presumibilmente, sempre più virtualizzate.

In *Second Life*[4] gli utenti vengono chiamati "cittadini" e per entrarvi è sufficiente accedere al sito di *Second Life* (www.secondlife.com), scaricare il programma ed installarlo sulla piattaforma.

A questo punto inizia una procedura di registrazione (durante la quale si dovranno accettare i termini e le condizioni poste), a cui seguirà la creazione di un *alter ego* virtuale che sarà presente nel gioco.

[3] Da Wikipedia: "il termine *Massive Multiplayer Online Role-Playing Game* ed il suo acronimo inglese MMORPG identifica un gioco di ruolo per computer o consolle che viene svolto tramite Internet contemporaneamente da più persone. Migliaia di giocatori possono interagire interpretando personaggi che si evolvono insieme al mondo che li circonda ed in cui vivono".

[4] Di qui in avanti si utilizzerà l'abbreviazione SL per riferirsi a Second Life.

Per utilizzare SL basta essere maggiorenni[5], possedere una carta di credito o un *account* Paypal ed avere una discreta conoscenza della lingua inglese.

Ci sono due possibilità per iniziare la vita su SL: una *basic*, completamente gratuita, l'altra da utente *premium,* sottoscrivendo un abbonamento mensile, trimestrale o annuale, pagabile con carta di credito, il quale ci consentirà di comprare terreni, costruire case nel mondo virtuale e mettere in piedi un'attività.

Già da questi primi passaggi si può intuire quindi come in SL la cittadinanza si acquisisca, per così dire, per *jus soli*, senza particolari formalità, se non quelle legate al possesso della carta di credito o dell'account Paypal.

Facendo riferimento all'utente di *Second Life*, dobbiamo prima dare una definizione fondamentale, quella di identità digitale, diversa da identità personale.

L'identità personale viene considerata come un complesso di dati anagrafici, utili a identificare un soggetto nei rapporti con i pubblici poteri e a distinguerlo dagli altri soggetti. La disciplina dell'identità digitale non ricorre invece in nessuna normativa vigente in quanto il codice dell'amministrazione digitale definisce soltanto le nozioni di carta d'identità elettronica e di firma digitale. L'identità digitale viene accostata all'identità in rete o virtuale, soprattutto per distinguere il corpo fisico da quello informatico.

2. Le transazioni in *Second Life*

All'interno di questo mondo virtuale esiste un'economia a sé stante, basata sui *Linden Dollars*, che si possono acquistare sul sito o direttamente su *Second Life* tramite carta di credito e sono convertibili in euro con un cambio di circa 1000L$ = 3 euro. Il cambio è soggetto a variazioni, proprio come nell'economia mondiale del mondo reale ed è gestito esclusivamente dalla società ideatrice di SL, la *Linden Labs*.

[5] Per un'età compresa invece dai 13 ai 18 anni vi è un'area apposita: la *Teen Area*. Sempre per un'età compresa fra i 13 e i 18 anni chi sottoscrive il contratto di adesione dichiara inoltre che i rispettivi genitori ne sono a piena conoscenza e i genitori stessi hanno letto e accettato le condizioni d'uso. Ai maggiori di 18 anni invece non è consentito l'accesso nelle *Teen Area*. Esiste poi un'altra area, quella *Adult only*, destinata ai maggiorenni e che può contenere materiale pornografico o scene violente.

Second Life è basato su una logica "*open source*"[6] dove gli utenti hanno a disposizione un linguaggio per costruire e personalizzare qualsiasi cosa. In pratica possono realizzare ogni genere di oggetti o di ambienti mediante l'acquisto o l'affitto di terreni virtuali dei quali la *Linden* riconosce la proprietà intellettuale ai creatori.

Nel corso del tempo, diverse comunità di utenti hanno creato luoghi (sim[7]) di ogni genere e ambientazione, ricostruzioni di città reali (es. Amsterdam), villaggi turistici, mall commerciali, gallerie d'arte e musei. Alcuni utenti hanno sviluppato un proprio business acquistando L$ (*Linden Dollars*) e rivendendoli quando avevano aumentato il loro valore, od acquistando oggetti o terreni e rimettendoli in vendita a prezzo più alto.

Moltissime aziende si sono affacciate su *Second life* per aprire un'attività, (Adidas, Ibm, Warner Bros, solo per citarne alcune); tra le aziende italiane vi è il gruppo "L'Espresso" che, dopo aver acquistato terreni, ha costruito la sua sede ove svolge l'attività di *branding* e *marketing,* ricorrendo all'organizzazione di eventi speciali che coinvolgono gli utenti.

Anche il leader dell'Italia dei Valori, Antonio di Pietro, ha aperto un punto informativo su *Second Life* per creare dibattiti con chiunque sia interessato. Il gruppo immobiliarista Gabetti ha aperto una sede con tanto di agenti immobiliari sottoforma di *avatar* che vendono terreni e fabbricati chiedendo in pagamento *Linden Dollars* (convertibili poi in veri euro).

Le transazioni in *Second Life* possono essere:

- Immobiliari (vendita di terreni virtuali e fabbricati, ricorrendo alle agenzie immobiliari virtuali);
- legate al gioco d'azzardo;
- vendita di oggetti virtuali per un uso commerciale (vestiti, personalizzazione del proprio *avatar*);

[6] Da Wikipedia: "termine inglese che significa sorgente *aperta* indica un *software* i cui autori (più precisamente i detentori dei diritti) ne permettono, anzi ne favoriscono il libero studio e l'apporto di modifiche da parte di altri programmatori indipendenti. Questo è realizzato mediante l'applicazione di apposite licenze d'uso".

[7] Il termine Sim sta ad indicare un simulatore di *Second Life*, ovvero la simulazione di una regione di 65536 metri quadri (256x256m). Corrisponde all'espressione comune "isola": tuttavia non tutti i sim hanno forma di isola; spesso invece le regioni sono connesse fra di loro formando *mainland* e continenti. Cfr. *amplius* http://www.secondlifeitalia.com/wiki/Sim.

- fornitura di servizi relativi a *Second Life* (progettazione di campagne di *marketing*, pubblicità);

A differenza di altri giochi *Second life* permette di fare acquisti, aprire imprese ed uffici, costruire, speculare e guadagnare. Le uniche regole su *Second Life* si trovano nel momento in cui si acconsente ai termini del servizio e alle regole del programma (previste sempre da *Linden Labs*).

Nel contratto di termini e condizioni ci sono 14 articoli e 17 allegati, nella maggioranza dei quali è la *Linden Labs* che decide a sua discrezione le sorti del gioco[8].

Nel regolamento si trovano alcuni comportamenti da tenere per il pacifico godimento dell'esperienza di "gioco", la tolleranza verso tutti gli altri utenti e la protezione della vita privata. Infatti ogni giocatore ha diritto alla sua vita privata ed ogni divulgazione di informazioni riservate, non volute dal giocatore, vengono considerate una violazione della *privacy*, della decenza e della tranquillità.

In caso di inosservanza di queste regole l'utente può essere escluso ed il suo *account*[9] eliminato; sono queste le uniche possibilità di protezione che possono avere gli utenti, mentre la *Linden* agisce come un governo autocratico. Naturalmente ci si aspetta che ogni utente tratti con rispetto gli altri, che non li molesti e che si attenga alle regole stabilite dalla *Linden*.

Giuridicamente la *Linden* è un *service provider* che, oltre a favorire l'accesso alla rete, offre anche ulteriori servizi, come la memorizzazione di pagine *web* e di archivi informatici, la conservazione di *files log*[10], ed altri.

[8] Esiste, a titolo esemplificativo, la *privacy policy*, la disciplina del gioco d'azzardo, la tutela del *copyright* e del marchio, la fatturazione in *Second Life*.

[9] Da Wikipedia: "Un *account* costituisce quell'insieme di funzionalità, strumenti e contenuti attribuiti ad un utente in determinati contesti operativi. In informatica, attraverso il meccanismo dell'*account*, il sistema mette a disposizione dell'utente un ambiente con contenuti e funzionalità personalizzabili. L'accesso ad un *account* è un processo chiamato login (o logon) ed associato ad una procedura di riconoscimento, detta autenticazione. Durante l'autenticazione, sono richieste le credenziali d'accesso, cioè lo *username* (nome utente) e la relativa *password* (parola d'ordine). Tali credenziali possono essere definite manualmente da un amministratore o generate automaticamente attraverso un processo di registrazione.

[10] Da Wikipedia: "termine usato con il significato di *giornale di bordo*, o semplicemente *giornale*, su cui vengono registrati gli eventi in ordine cronologico". Il termine è stato importato nell'informatica per indicare: la *registrazione cronologica* delle operazioni man mano che vengono eseguite e il *file* su cui tali registrazioni sono memorizzate.

3. La responsabilità dei *provider* in Italia

Il legislatore italiano, per fornire un minimo di regole, ha disposto con il d.lgs. 70/03[11] una differenziazione delle attività svolte dai prestatori di servizi chiarendo, solo in parte, alcune responsabilità.

Sono individuabili tre principali categorie di operatori telematici. La prima riguarda i "connection provider" (o Isp), vale a dire quei soggetti che forniscono agli utilizzatori di Internet l'accesso alla Rete. Vi sono poi i *server provider*, i quali mettono a disposizione uno spazio di memoria sui siti Internet. Normalmente le due figure appena delineate coincidono. La terza categoria interessa i *content provider*, vale a dire una categoria eterogenea di soggetti che forniscono la documentazione elettronica caricata su un sito affinché possa essere visualizzata. Si possono ricordare, tra gli altri, gli autori delle opere multimediali, chi scrive *e-mail* o messaggi ovvero partecipa, ad esempio, a gruppi di discussione[12].

E proprio in ragione dell'attività svolta dai prestatori il legislatore ha ritenuto di dover diversificare le responsabilità di cui ai tre articoli sopra menzionati[13].

Si è così inquadrata, all'art. 14, la figura di *mere conduit*, consistente nel servizio di mero trasporto delle informazioni, si pensi ai servizi di accesso alla rete che consentono la trasmissione di informazioni. In questo caso per il prestatore, in via generale, vige l'assenza di un obbligo di verifica del contenuto delle informazioni. Queste vengono memorizzate, o trasmesse sui propri *servers* e si subordina la responsabilità alla sussistenza di diverse condizioni, quali l'aver originato la trasmissione, l'aver selezionato il destinatario della trasmissione oppure aver selezionato o modificato le informazioni trasmesse.

Nel caso disciplinato dall'art. 15, invece, relativo all'attività di *caching*, si è esclusa la responsabilità del *provider* in ordine alla memorizzazione auto-

[11] D.lgs. 9 aprile 2003, n. 70, *Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno*, in G.U. 14.04.2003 S. O. n. 61.

[12] Cfr. C. Gattei, *Tutela dell'opera multimediale su rete telematica: la situazione europea*, in "Diritto dell'Informazione e dell'Informatica", 1998, n. 2, pp. 469 e ss.

[13] L. Nivarra, *La responsabilità degli intermediari*, in "Aida", XI, 2002, pp. 308 e ss.

matica e temporanea effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta.

L'esclusione della responsabilità, ad ogni modo, è condizionata al rispetto di cautele ed obblighi da parte del *provider*, così come previsto dal considerando 33 della direttiva 2000/31/CE[14], sostanzialmente riassumibili nel divieto di modificare le informazioni veicolate, nell'obbligo di rimuovere prontamente le informazioni una volta che il fornitore del servizio sia stato messo al corrente della loro illiceità, nell'astenersi dal compromettere l'uso della tecnologia diffusa in quel dato momento per risalire alle destinazioni delle informazioni, nel disabilitare l'accesso o rimuovere le informazioni su ordine dell'autorità amministrativa o giudiziaria.

All'art. 16, che disciplina l'attività di memorizzazione permanente (*hosting*) è previsto che il *provider* sia responsabile delle informazioni lesive di altrui diritti se era al corrente che l'attività o l'informazione erano illecite o di fatti o circostanze che non rendevano manifesta l'illegalità dell'attività o dell'informazione o se, non appena al corrente di tali fatti, non abbia agito immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

Già la giurisprudenza di merito aveva escluso la responsabilità del provider "che si limiti a ospitare sul proprio *server* una tabella di informazioni caricatavi da un proprio cliente, e costituente violazione di un altrui diritto d'autore"[15].

È netta poi la distinzione tra la responsabilità preventiva e quella successiva del *provider*. La prima è limitata ai *service provider*, mentre la seconda è riferibile a qualsiasi tipologia di *provider* attribuendo a questi soggetti la responsabilità di non aver bloccato l'aggravamento dei danni derivanti dal comportamento illecito di alcuni utenti.

Il d.lgs. 70/2003 sancisce l'assenza dell'obbligo di sorveglianza del "*provider*": all'art. 17 dispone che il prestatore di servizi non è assoggettato ad un obbligo di sorveglianza sui contenuti che circolano o che memorizza e a ricercare le informazioni che denotino comportamenti illeciti.

[14] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000, Relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico").

[15] Trib. Cuneo 23.6.97, in "Aida", 1997, pp. 500 e ss.

Inoltre, mancando un obbligo di sorveglianza, non pare applicabile neanche l'art. 40 c.p. ("Non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo") che specifica come unico obbligo del prestatore di servizi sia quello di informare tempestivamente l'autorità giudiziaria o quella amministrativa, identificando, o permettendo di identificare, il proprio cliente.

Invece è prevista la responsabilità del *provider* qualora, su richiesta espressa dell'autorità giudiziaria o amministrativa, abbia in qualche modo ritardato la rimozione dei contenuti illeciti, ovvero, essendo a conoscenza di informazioni illecite, non abbia informato l'autorità competente.

Viene così ribadita la caratteristica di neutralità dei *provider*s rispetto alle informazioni che circolano in rete, così, apparentemente, esenti da responsabilità oggettiva.

La responsabilità penale del *service provider* si verifica esclusivamente con riferimento alle aree pubbliche, qualora un utente diffonda informazioni o contenuti illeciti in spazi destinati al pubblico dominio e di competenza del *service provider*.

In tal caso non vi sarebbe una responsabilità oggettiva del *provider* né una responsabilità di sorveglianza, ma solamente l'onere di rimuovere tempestivamente i contenuti illeciti che circolino nelle "aree pubbliche". La figura professionale del *provider* non pare assoggettabile per analogia a quella del direttore di una testata giornalistica, ovvero a quella dell'editore televisivo.

Contrariamente all'area pubblica, opinione maggioritaria della dottrina è che nella comunicazione privata (*email*) e nei servizi di messaggistica (anche su *Second Life*) non si possa ipotizzare alcuna forma di responsabilità penale del *service provider*, in quanto su di essa non potrebbe esercitarsi alcuna attività legittima di controllo o censura in forza del combinato disposto degli artt. 15 e 21 della Costituzione , che sanciscono la libertà e la segretezza della corrispondenza, nonché la libera manifestazione del proprio pensiero.

Premesso quanto sopra è doveroso osservare che per garantire misure idonee di sicurezza sarebbe onere del *provider* identificare, senza margini di errore, ogni utente che interagisca con la rete, così da frenare il proliferarsi dei crimini informatici e da diventare un valido deterrente nei confronti di quella categoria di utenti che utilizzano la rete per fini illeciti.

Inoltre, l'identificazione sicura dell'utente provocherebbe un duplice risultato: quello di garantire alla vittima degli illeciti una possibilità di

risarcimento dei danni subiti e subendi e quello di evitare che il *provider* venga tramutato in un "capro espiatorio" di qualunque illecito compiuto utilizzando la rete.

4. La responsabilità dei *provider* negli USA

La scelta, sia a livello europeo, sia nazionale, di non considerare responsabili i *provider* è frutto della considerazione che l'intermediario di servizi Internet di accesso, è assimilabile al ruolo svolto da una compagnia telefonica (*carrier*) e, quindi, non responsabile dei contenuti di una eventuale comunicazione digitale lesiva di diritti. Questa conclusione si ricollega ad altra analoga cui si è pervenuti oltreoceano con una pronuncia USA della Corte Suprema del 2000.

In tale occasione, relativa ad un caso di diffamazione a mezzo Internet, il collegio ha confermato la sentenza della Corte d'appello dello Stato di New York, secondo la quale il *provider* (Prodigy) è stato il semplice veicolo attraverso cui è transitato il messaggio offensivo. Sicché avendo un ruolo passivo, vale a dire non essendo l'autore del reato, assimilabile a quello di una compagnia telefonica, non è stato riconosciuta la sua responsabilità in ordine ai contenuti della comunicazione digitale offensiva[16].

La sentenza del 2000 della Corte Suprema americana, stabilendo che un *provider* non possa essere responsabile dei messaggi apparsi sui *newsgroup*[17] ospitati dai propri *server*, diventa così un caso internazionale applicabile anche all'universo di *Second Life*.

Ma la Corte Suprema ha confermato la sentenza già emessa dalla Corte d'Appello dello Stato di New York secondo cui Prodigy[18] ha un

[16] Sul punto v. l'url: http://www.tin.it/ notiziapiu/new// 170798_provider_soc.html.

[17] Da Wikipedia: "uno degli spazi virtuali creato su una rete di *server* interconnessi per discutere di un argomento (*topic*) ben determinato. In italiano a volte viene utilizzato il termine gruppo di discussione".

[18] Nel caso di specie *Prodigy*, uno dei principali *provider* statunitensi, è stato citato in tribunale perché non avrebbe fatto abbastanza per fermare un utente che, spacciandosi per un ragazzo, ha inviato messaggi ed *email* con contenuto osceno ad un *boy scout*. Il ragazzo "vittima" delle *email* false, Alexander G. Lunney, insieme al padre, si è appellato alla Corte Suprema degli Stati Uniti per vedere condannato *Prodigy*, visto che i messaggi contenenti termini offensivi e illeciti erano stati inviati dai suoi *server*.

ruolo passivo di veicolo per i messaggi e, proprio come una normale azienda telefonica, non può essere denunciato per il suo servizio[19].

Il *provider* quindi non avrebbe il dovere di sorvegliare né le relazioni tra utenti né quelle con i servizi offerti avendo un controllo estremamente limitato anche se conserva un controllo su qualità, sicurezza, moralità, veridicità ed accuratezza del servizio offerto. È possibile infatti segnalare alla *Linden Labs* comportamenti scorretti di cui un *avatar* è stato vittima, tramite un apposito comando; la *Linden* provvederà alla pubblicazione su un apposito sito internet dei provvedimenti presi in caso di abuso.

Una delle regole riguardanti gli *avatar* è che ogni singolo *account* possa essere usato da un'unica persona. Ad un *avatar* quindi deve corrispondere solo un individuo ma, al contrario, una persona fisica può avere più *avatar*, nulla vieta infatti che si possano creare e far agire due *avatar*[20]. Un *avatar* non può essere ceduto ad altre persone se non dietro permesso della *Linden*. Quest'ultima fa valere una specie di testamento: se un iscritto decide di non usare più un *account* può lasciare in eredità tutti i beni acquisiti, la *Linden* gestirà la cosiddetta "successione" senza prevedere, almeno per ora, tasse da pagare.

5. Il diritto tributario in SL

Second Life ha attratto milioni di uomini e di donne da ogni parte del mondo, per alcuni è un mondo virtuale dove poter vivere una seconda vita,

[19] Per la verità il tema dell'irresponsabilità dei provider non è sempre stato così pacifico. Nel 1995 la stessa *Prodigy* fu invece condannata per un caso di diffamazione a mezzo internet. In tale occasione la Corte di New York ha statuito il principio che l'ISP può essere citato in giudizio per rispondere dei danni causati da un atto diffamatorio come se si trattasse di una televisione, un giornale ovvero un editore. Nel caso di specie la Stratton Oakmont Inc. società di consulenza finanziaria aveva citato in giudizio *Prodigy* asserendo di essere stata denigrata da una serie di messaggi pubblici apparsi in un forum finanziario in cui si asseriva che il presidente della Stratton era stato incriminato per vari reati. La *Prodigy* si era difesa sostenendo che, nella sua qualità di distributore non poteva essere chiamata a rispondere di azioni intraprese da terzi, e ciò anche perché non aveva alcun controllo sulle notizie pubblicate. In giudizio fu invece appurato che *Prodigy* operava un controllo, seppur parziale, sui contenuti della messaggistica pubblica attraverso agenti *software* che provvedevano ad eliminare tutti i messaggi osceni.

[20] Degno di menzione è il fatto che in alcuni Paesi l'utente maschio che impersoni un *avatar* di sesso femminile rischi il carcere.

per altri è il più grande videogioco di tutti i tempi, ogni ora le creature digitali che animano le strade e le isole di *Second Life* spendono milioni di dollari americani in bit, poligoni tridimensionali, forme e proprietà intellettuali.

Second Life è diventato anche teatro di illeciti: in questo mondo ogni giorno si scambiano merci e si cedono diritti di proprietà intellettuale per milioni di dollari *Linden* e quindi centinaia di migliaia di dollari o euro, si sfornano notizie suscettibili di influenzare l'andamento dei mercati, si stringono relazioni interpersonali e commerciali, si sconfina nell'illegalità con il gioco d'azzardo e la pedo-pornografia.

Tutto questo è affidato solo ed esclusivamente alle regole dettate dalla *Linden Labs*, proprietaria di un paese virtuale, che ha raggiunto un *pil* superiore a quello di molti paesi del mondo ed una popolazione di milioni di persone.

Si verificano anche atti di vandalismo con distruzione di poligoni tridimensionali rappresentanti auto, abitazioni e vetrine, rapimenti, usura ai commercianti: è difficile pensare che le sole regole del contratto garantiscano la legalità. In SL si commercializza ormai ogni genere di prodotto o servizio lecito o illecito, tutto questo senza che nessuno Stato possa rivendicare l'appartenenza di SL al proprio territorio.

In Italia i possibili guadagni ottenuti da *Second Life*, dal momento in cui i soldi vengono trasferiti dal mondo virtuale ad un conto corrente (con operazione di conversione di valuta *Linden Dollar*/euro) dovrebbero essere tassati, secondo quanto previsto dalla nostra Costituzione all'art. 53 (t*utti sono tenuti a concorrere alle spese pubbliche in ragione della loro capacità contributiva*).

Le tasse andrebbero pagate sui "Redditi" prodotti.

Un flusso di denaro (reale) proveniente da una qualunque attività (anche virtuale) è pur sempre un reddito.

A seconda della posizione fiscale sarà diversa la tassazione. Se l'utente di *Second Life* nella vita reale è un lavoratore dipendente dovrà inserire i redditi (i soldi trasformati da *Linden Dollars* in euro) nel 730 sotto la voce "Altri redditi". Se solitamente non viene redatto il 730, bisogna farlo appositamente per sommare questi redditi ai redditi da lavoro dipendente. Se l'utente è un lavoratore autonomo dovrà invece inserire i redditi (i soldi trasformati da *Linden* in euro) nel modello UNICO sotto la voce "Altri redditi".

Se l'utente è a carico di altri soggetti (es. genitori) saranno questi ultimi a dover indicare i redditi tra quelli dei membri del nucleo familiare o tra gli Altri Redditi nelle proprie dichiarazioni dei redditi (730 o UNICO).

6. La a-territorialità di *Second Life*

L'assenza di un preciso riferimento territoriale rappresenta uno dei maggiori problemi da affrontare nell'interrogarsi sull'opportunità e la possibilità di estendere anche a *Second Life* le regole del mondo reale e tradizionale. Non è solo il territorio a mancare, mancano anche i cittadini, volendo fare riferimento a persone in carne e ossa e con un patrimonio di riferimento a garanzia delle obbligazioni da essi assunte.

Troppo spesso gli *avatar* che agiscono in *Second Life* sono solo astratte proiezioni dell'immaginazione di uomini e donne che omettono di farsi riconoscere con il proprio nome e cognome o nazionalità.

L'*avatar* è da considerarsi come un mero prolungamento della personalità dell'individuo che lo anima e non un rappresentante in senso tecnico (art 1387 c.c.) poiché non si può configurare in alcun modo, in capo all'*avatar*, il concetto di persona giuridica o persona fisica. L'*avatar* è dunque un mero strumento, una trasposizione di sé stessi all'interno del mondo virtuale, (in poche parole un'immagine ideale). Nessuno può certificare con certezza chi si trovi dietro il personaggio fatto di pixel, la certezza della paternità delle azioni, della persona che anima l'*avatar* perché non è garantita da un sistema di riconoscimento univoco (ad esempio tramite un codice fiscale e un sistema a doppia chiave asimmetrica utilizzato dai certificatori per la firma digitale, così come previsto dal d.lgs. 82/2005[21]).

Quindi vi sono parti che stipulano contratti fra di loro e svolgono la relativa prestazione senza conoscere esattamente l'identità della controparte.

Attraverso la piattaforma SL sono molteplici le fattispecie di diritto a cui un *avatar* va incontro. Potrebbero rientrare nella categoria dei contratti telematici quei contratti stipulati mediante un sistema telematico, nel caso il *browser* di SL, senza che le parti debbano essere presenti nello stesso luogo e nello stesso tempo.

[21] D.lgs. 7 marzo 2005, n. 82, *Codice dell'amministrazione digitale*, pubblicato in G.U. del 16 maggio 2005, n. 112 - S.O. n. 93.

La capacità di SL è di proporre fattispecie di diritto finora impensabili dal punto di vista telematico: non solo la compravendita di terreni e di spazi virtuali su *server* che vengono considerati come luoghi, ma anche la possibilità di dare in locazione un determinato luogo a fronte del pagamento di un canone mensile riporta alla mente un universo certamente virtuale ma molto più simile alla *Real Life* di quanto la rete non abbia mai permesso. Ovviamente non stiamo parlando di contratti di compravendita o di locazione veri e propri, dato che non c'è alcun bene fisico su cui creare o modificare diritti reali, e soprattutto è impossibile registrare presso alcuna pubblica autorità la compravendita effettuata (comportamento invece obbligatorio in caso di *Real Life*). Vero è, dunque, che non si tratta di vera compravendita di terre o locazione delle stesse, ma occorre comunque notare che si possono configurare delle problematiche legate a questo genere di contratti.

Elemento fondamentale della dottrina del contratto è certamente la formazione dell'accordo, l'incontro delle volontà contrattuali e il modo in cui queste volontà vengono espresse dai contraenti stessi. La dottrina analizza una fondamentale fattispecie che caratterizza l'impossibilità per le parti di concludere una negoziazione stando fisicamente una in prossimità dell'altra: la notifica dell'accettazione. Secondo l'art. 1326 c.c., infatti, il contratto si ritiene concluso nel momento in cui la parte proponente viene a conoscenza della volontà, espressa o tramite comportamento concludente, dell'altra parte, di accettare: "Il contratto è concluso nel momento in cui chi ha fatto la proposta ha conoscenza dell'accettazione dell'altra parte. [..] Un'accettazione non conforme alla proposta equivale ad una controproposta".

SL pone lo stesso problema che viene posto da qualunque altro strumento di ricezione a distanza di questa volontà e cioè ci si chiede quando questa conoscenza si possa presumere e in quale occasione possa essere impugnata come erronea dalla parte accettante che accettante non vuol essere per nulla, senza contare il rischio di un comportamento concludente male interpretato: con il *browser*[22] sembra non esserci tempo a suf-

[22] Da Wikipedia: "(in italiano: *navigatore*) è un programma che consente agli utenti di visualizzare e interagire con testi, immagini e altre informazioni, tipicamente contenute in una pagina *web* di un sito.

ficienza per la revoca, poiché la notifica dell'accettazione è pressoché immediata e quindi il contratto si perfeziona immediatamente.

Altra tematica di interessante rilievo giuridico riguarda il luogo di formazione del contratto, fondamentale soprattutto alla luce del fatto che normalmente tale luogo è in grado di definire la normativa che a quel contratto sarà applicata.

La dottrina pretende che al contratto sia applicata la normativa del luogo in cui esso è stato concluso, generalmente assumendo come luogo di formazione del contratto quello in cui il proponente ha ottenuto notizia dell'accettazione della controparte.

A fronte di due tesi superate, che pretendevano che il contratto si considerasse formato dove il ricevente scaricava la posta elettronica che gli dava notizia dell'avvenuta accettazione (in questo caso) con il *browser* di SL, presso il computer che fisicamente sta utilizzando il *browser*, o il luogo dove risiedevano i *server* preposti alla ricezione telematica. Visto e considerato che i *server* della *Linden* risiedono tuttora esclusivamente in California, in ogni caso, dovrebbe applicarsi la normativa americana. Ad oggi la maggior parte della dottrina concorda nel sostenere che il luogo di conclusione del contratto vada ravvisato nel luogo in cui il ricevente svolge la propria attività professionale o ha il polo principale di interesse per la sua attività: non conoscere la reale identità del soggetto con cui si stipula il contratto può divenire davvero rischioso.

Un caso riguardante l'acquisto di terreni degno di menzione è quello dell'avvocato americano Marc Bragg, che ha citato in giudizio la società *Linden Labs* – prima di fronte a un giudice della Pennsylvania e ora davanti ad una Corte federale – per ottenere un risarcimento danni. Oggetto del contendere erano alcuni lotti di terreno virtuale acquistati da Bragg in SL e successivamente sequestrati dai *Linden Labs* (LL), apparentemente senza motivo e senza che sussistesse una palese contravvenzione al regolamento che ogni utente deve accettare al momento della creazione del proprio *account*.

In realtà però la vicenda è più complessa di quel che sembra. Stando a quanto dichiarato dall'avvocato, infatti, la società di San Francisco avrebbe violato di fatto le leggi della Pennsylvania a tutela dei consumatori disattivando senza preavviso il suo *account*, e facendogli così perdere la proprietà dei terreni acquistati all'asta in SL. Terreni che Bragg avrebbe potuto rivendere con notevole profitto, poiché erano stati da lui rilevati "a un prezzo molto

conveniente, in quanto decisamente inferiore a quello di mercato". In pratica, gli amministratori di SL avrebbero dapprima consentito la messa all'asta dei terreni, quindi incassato i dollari (veri) spesi dall'utente per l'acquisto, provvedendo poi illegittimamente all'azzeramento del conto, causandogli un evidente danno. Le richieste di rimborso del denaro reale speso dall'avvocato per l'acquisto della terra virtuale sono state ignorate dai LL, ed è per questo motivo che l'uomo ha optato per il ricorso alla giustizia del mondo reale.

Dal canto loro i *Linden Labs* si sono difesi di fronte al giudice sostenendo che l'avvocato fosse entrato in possesso dei beni virtuali in questione secondo un procedimento non regolamentare e quindi non valido. Ma tale difesa non ha convinto la Corte, che ha passato la questione al tribunale federale. Per la prima volta, quindi, sarà la legge statunitense, non quella dei *Linden*, a stabilire chi – e in quali termini – abbia il diritto di disporre di un bene virtuale acquistato con denaro vero all'interno di quello che tecnicamente è solo un gioco *multiplayer*[23] *online*. Perché, sostiene Bragg, se da un lato è vero che nulla di ciò che si trova all'interno di SL esiste, dall'altro è vero anche che i *Linden Labs* sono comunque obbligati a onorare le leggi che regolano il contratto e la compravendita nel mondo in cui viviamo.

7. Le ODR (*Online Dispute Resolution*) in *Second Life*

Dal punto di vista processuale, ancora una volta la definizione del luogo di conclusione del contratto è fondamentale per definire anche quale giurisdizione sia competente nella decisione di un'eventuale controversia, per quanto spesso questo problema venga risolto con la definizione volontaria fra le parti.

A tale proposito il TOS[24] del 2010 prevede che, nel caso di controversia tra l'utente e *Linden Lab* in merito a una richiesta il cui valore sia inferiore a 10.000 USD dollari, la questione possa essere risolta tramite arbitrato, anziché con un procedimento contenzioso.

[23] Da Wikipedia: "in italiano, multigiocatore: un termine utilizzato nel mondo dei videogiochi per indicare la modalità di gioco in cui più persone possono giocare allo stesso gioco nello stesso momento utilizzando lo stesso o, più spesso, diversi terminali (computer) collegati tra loro.

[24] *Terms of Service*, recentemente modificato nell'aprile 2010, è rinvenibile all'url http://secondlife.com/corporate/tos.php.

Così all'art 12.1. del TOS 2010 è prevista la facoltà di ricorrere ad un arbitrato vincolante formulato da un collegio arbitrale scelto dalle parti di comune accordo.

Sia l'arbitro sia le parti devono però rispettare le seguenti regole:

(a) l'arbitrato è condotto, a scelta della parte che chiede aiuto, per telefono, *online* o basato esclusivamente su osservazioni scritte,

(b) l'arbitrato non comporta alcuna comparizione personale delle parti o dei testimoni se non diversamente concordato dalle parti, e

(c) il giudizio sul lodo reso dall'arbitro può essere fatto valere in qualsiasi tribunale competente.

D'altra parte, qualora non ci si avvalga di questa particolare ADR *Linden* Labs avvisa l'utente che i rapporti sono disciplinati dalle leggi dello Stato della California, senza riguardo al conflitto dei principî del diritto o della Convenzione delle Nazioni Unite sulla vendita internazionale di merci. Inoltre, l'utente e *Linden Lab* accettano di sottoporsi alla giurisdizione esclusiva dei tribunali situati nella Città e Contea di San Francisco, California, salvo quanto previsto nel caso di arbitrato. Nonostante ciò, ciascuna parte ha la possibilità di richiedere altre ingiunzioni o un giusto indennizzo per proteggere diritti di proprietà intellettuale in qualsiasi tribunale competente in cui l'altra parte risiede o ha la sua sede principale[25].

8. I CRM (*Customer Relationship Management*) e *privacy*

Il CRM[26] (*Customer Relationship Management*) è un insieme di programmi di gestione delle relazioni coi clienti reali o potenziali offerto da aziende di *marketing* alle imprese, come nel nostro caso *Second Life*.

[25] Art. 12.2. Tos Second Life, rinvenibile all'url: http://secondlife.com/corporate/tos.php. "You agree that this Agreement and the relationship between you and Linden Lab shall be governed by the laws of the State of California without regard to conflict of law principles or the United Nations Convention on the International Sale of Goods. Further, you and Linden Lab agree to submit to the exclusive jurisdiction and venue of the courts located in the City and County of San Francisco, California, except as provided in Section 12.1 regarding optional arbitration. Notwithstanding this, either party shall still be allowed to apply for injunctive or other equitable relief to protect or enforce that party's Intellectual Property Rights in any court of competent jurisdiction where the other party resides or has its principal place of business".

[26] Da Wikipedia: "(Gestione delle relazioni con la clientela) Servizi che utilizzano metodologie comprovate e tecnologie di e-business per offrire alle aziende l'opportunità di identificare,

È un concetto legato alla fidelizzazione dei clienti; in un'attività come quella dei *Linden Labs* il mercato non è rappresentato solo dal cliente ma anche dalla capacità dell'impresa di stabilire relazioni durevoli di breve e lungo periodo cercando non solo di mantenere i suoi utenti ma anche di trovarne di nuovi.

Si tratta in definitiva di un sistema per l'analisi e la gestione della relazione con gli *avatar* che consente di monitorare con precisione le azioni di *marketing* ed i ritorni economici all'interno delle isole di SL. Negli eventi organizzati da Metaverse CRM (società che si occupa di CRM per conto di *Linden Labs*) si sono sollevati una serie di interrogativi connessi alla tutela della *privacy* dei soggetti coinvolti in SL. A tal proposito, ad esempio, ci si chiede come trattare le conversazioni tra *avatar,* oggetto di controllo da parte della società di CRM.

Sembra opportuno, a tal proposito, predisporre un'informativa da sottoporre e far accettare all'utente al momento della raccolta dei dati personali, siano essi dati comuni o sensibili, o conversazioni tenute su *Second Life*, indicando ai sensi dell'art. 13 del Codice della *privacy* (d.lgs. 196 del 2003[27]):

- finalità e modalità del trattamento;
- natura obbligatoria o facoltativa del consenso;
- conseguenze di un eventuale rifiuto da parte dell'utente;
- ambito di diffusione dei dati;
- estremi identificativi del titolare del trattamento dei dati e degli eventuali responsabili da lui nominati.

Poiché il CRM è in grado di tracciare qualunque tipo di comportamento all'interno dell'isola, l'unica conseguenza configurabile a fronte di un rifiuto a corrispondere il consenso al trattamento dei dati è l'impossibilità di entrarvi.

9. I Reati su *Second Life*

I crimini ordinari possono essere commessi anche con l'utilizzo di strumenti informatici ma questa è solo una possibilità, non un requisi-

selezionare, acquisire, sviluppare e trattenere i clienti profittevoli, costruendo relazioni salde, fondamentali per garantire un successo a lungo termine".

[27] D.lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123.

to necessario; i crimini informatici invece sono quelli commessi per mezzo di – o su – strumenti informatici e tale requisito viene considerato necessario[28].

Per quanto riguarda invece i crimini virtuali, essi non possono considerarsi veri e propri crimini ma piuttosto situazioni della realtà virtuale che non provocano una vera e propria offesa individuabile in ambito giuridico, ma recano comunque in sé un certo disvalore giuridico.

Second Life detta alcune regole che proibiscono determinati comportamenti prevedendo sanzioni che passano dall'avvertimento, alla sospensione temporanea dell'*account,* fino ad arrivare al *banning,* cioè a bandire l'utente.

La mancanza di una vera e propria legislazione non è un problema da sottovalutare in quanto all'interno di questo mondo virtuale esistono rapporti giuridici riconducibili al mondo reale, basti pensare all'acquisto di terreni, sottoposto nel nostro ordinamento al diritto privato.

Nel 2008 un reporter di una TV tedesca, Nick Schader, ha pubblicato i risultati di una sua inchiesta che fa conoscere uno dei lati oscuri di *Second Life* cioè la pedofilia. Inquietante il fatto che fare sesso virtuale con un bambino costa solo 500 *Linden Dollar* cioè neppure due euro.

Il reporter, fingendosi interessato all'argomento, entra in contatto con un gruppo di utenti e cerca filmati ed immagini pedopornografiche. Al reporter venivano offerti due tipi di servizi: incontri ravvicinati in angoli appartati di SL con *avatar* dalle sembianze infantili oppure la possibilità di ricevere via *e-mail file* digitali con protagonisti bambini veri. In questo caso ovviamente il prezzo era più alto.

La *Linden Labs* ha cercato di difendersi attraverso un comunicato, pubblicato nella *home page* del sito, affermando che anche se è vero che nelle comunità virtuale si possono fare cose quasi infinite, non saranno permesse e tollerate immagini reali, *avatar* od altre rappresentazioni che coinvolgano minori in scene a sfondo sessuale o violenza.

Per tentare di arginare il fenomeno la polizia di Vancouver ha inventato una divisione speciale operante su *Second Life*. In Germania la pedofi-

[28] Tali crimini sono per esempio quelli derivanti dalla frode informatica regolata anche dal nostro codice penale all'art. 640-*bis*, o l'accesso abusivo a sistema informatico o telematico di cui all'art. 615-*ter* c.p.

lia virtuale viene considerata un crimine e due utenti che detenevano materiale proibito sono stati identificati dai *Linden Labs* e rischiano fino a cinque anni di reclusione.

Un modo per bloccare sul nascere la pedofilia virtuale potrebbe essere quello di impedire, tramite *software* che un *avatar* adulto possa avere rapporti sessuali con un *avatar* bambino. Al momento alla *Linden Labs* nessuno ci ha pensato. Certo non si fermerebbero le immagini aventi per oggetto bambini "Real"però si limiterebbero i rapporti sessuali a soli adulti consenzienti.

10. I furti di identità

Un caso emblematico che fa riflettere è accaduto in SL: due *avatar* si sposano fra loro nella comunità virtuale, trascorso un po' di tempo si rendono conto che il loro rapporto non funziona ed il marito chiede il divorzio. Lei, ferita e risentita entra in *Second Life* con le sembianze dell'ex marito, rubandogli i dati di accesso e decide di distruggere "l'*alter ego* virtuale" del suo compagno *on-line*.

La donna viene davvero arrestata ed attende un processo reale che potrebbe condannarla ad una multa di 5.000 dollari, rischiando fino a cinque anni di carcere in quanto avrebbe commesso, per gli USA, un reato federale per furto di identità.

Occorre sottolineare che non sono rari negli USA ed in Giappone i casi che avvengono nel mondo virtuale e vengono poi portati sotto il controllo ed il giudizio della polizia e magistratura reale. Vi sono già state alcune condanne come nel caso di due ragazze che avevano rubato in SL e sono state perciò condannate dal giudice a lavori sociali in *Real Life,* per espiare la colpa di un fatto avvenuto in un mondo virtuale.

Altro caso di reato commesso nel mondo virtuale è quello di un ragazzo olandese di 17 anni che con l'intento di far vivere il proprio personaggio all'interno del gioco una vita piacevole senza però spendere nulla ha pensato bene di violare gli *account* di altri giocatori e rubare loro tutto ciò che gli serviva, il tutto per un valore complessivo di circa 4.000 euro. Tale condotta integra indubbiamente gli estremi del furto che riguarda sia gli oggetti virtuali, sia le informazioni personali degli utenti. Può stupire il fatto che qualcuno venga arrestato per aver rubato qualcosa di intangibile, ma non deve sorprende il fatto che la polizia intervenga qualora ravvi-

si la messa in atto di uno "*scam*"[29], vale a dire un business realizzato tramite pratiche fraudolente da parte di un internauta.

I furti di informazioni personali sono un problema. In passato si sono verificati altri casi analoghi ma è la prima volta che la polizia interviene. Si tratta di un furto reale perché i beni rubati erano stati pagati con denaro reale.

11. Il *COPY BOT*

Il meccanismo che differenzia profondamente il mondo di *Second Life* dagli altri MMORPG in cui ogni oggetto è di proprietà dello sviluppatore, è il fatto che ai suoi abitanti sia riconosciuto il diritto di rivendicare il *copyright* sulle proprie creazioni, di venderle o di opporsi alla crescita o alla copia.

Anche in materia di diritti di proprietà intellettuale, in particolare relativamente all'uso di marchi e loro contraffazione, si sono create situazioni controverse portate in giudizio. Dato il progressivo sviluppo ed il crescere del valore delle attività sviluppate in *Second Life*, l'interesse da parte di alcuni di contestare la posizione della *Linden Labs* e di far valere le proprie ragioni in Tribunale è sempre maggiore. C'è da un lato il problema di attribuire la titolarità dei diritti di proprietà intellettuale sui beni creati in SL, dall'altra si pone il problema della contraffazione, basta infatti entrare nel mondo virtuale per capire come i marchi e le griffe che si trovano nel mercato "reale" siano spesso imitati e venduti utilizzando la moneta virtuale (il *Linden Dollar*).

Proprio per tutelare la proprietà intellettuale è stato creato il CopyBot, un'applicazione sviluppata da *Libsecondlife*, un gruppo che collabora con *Linden Labs*, per scovare errori del sistema del mondo virtuale che potrebbero esser sfruttati con intenti malevoli. CopyBot era nato come applicazione per consentire il *backup*, prima di essere modificato da un utente ed essere rivenduto come macchina per clonare. CopyBot rappresenta una seria minaccia alle attività, dato che consente a chiunque, e non

[29] Da Wikipedia: "termine che indica un tentativo di truffa con i metodi dell'ingegneria sociale, effettuato in genere inviando una e-mail nella quale si promettono grossi guadagni in cambio di somme di denaro da anticipare. Spesso scam e spam sono strettamente correlati".

solo ad esperti programmatori, di replicare oggetti e rivenderli, violando quindi il *copyright* che viene loro riconosciuto da *Linden*.

12. Le contraffazioni e il *copyright*

Second Life è nata con l'idea di esaltare la creatività dei suoi residenti che, attraverso strumenti più o meno complessi, hanno avuto la possibilità di produrre e rivendere le proprie creazioni. La comunità si è perciò arricchita di costruzioni virtuali, opere d'arte e di architettura. In pratica non esiste nessun settore della creatività umana che non abbia un riproduzione virtuale.

Anche SL non è immune dal problema della contraffazione: è possibile imbattersi in negozi molto frequentati che vendono a caro prezzo modelli realizzati con *texture*[30] rappresentanti animali, composizioni architettoniche, decorazioni o fregi. Se tali oggetti fossero il frutto di creatività e talento personali non ci sarebbe nulla di strano nel rivenderli ottenendo un giusto guadagno ma ci si può anche imbattere in personaggi privi di scrupoli che perpetrano truffe ai danni di ingenui clienti che pagano di tasca propria prodotti risultati poi rubati. Creare un falso è semplice: in pratica è sufficiente ridurre alla forma di *texture* il modello stesso e quindi importarlo in questa forma in SL.

Fino a quando tali prodotti sono destinati ad un uso personale non si presentano problemi, tuttavia rivenderli rappresenta un arricchimento indebito che non tiene conto delle licenze d'uso e le normali condizioni di *copyright*. Basta controllare come vicino a tutte le riproduzioni offerte da questi siti specializzati si evidenzi la scritta: "modello per ricerca, è vietato l'uso di qualsiasi iniziativa commerciale".

Risulta invece che in SL esistano fiorenti attività commerciali che dalla vendita di materiale coperto da licenza si sono arricchite approfittando della buona fede di molti che hanno creduto invece di trovarsi di fronte a geni del settore.

Come detto dal 30 aprile 2010 sono entrati in vigore i nuovi ToS (*Terms of Service*), che regolano l'utilizzo di *Second Life*.

[30] Da Wikipedia: "immagine utilizzata per rivestire la superficie di un oggetto virtuale, tridimensionale, o bidimensionale, con un apposito programma di grafica".

Fra le novità di rilievo figura la *Snapshot and Machinima Policy*, una sezione dei ToS espressamente dedicata a bilanciare le esigenze di fotografi e *videomaker* con quelle – relative a *privacy* e *copyright* – degli utenti in generale.

La nuova *policy* distingue fra fotografie (*snapshots*) e video (*machinima*), probabilmente sulla base del fatto che un video risulta più invasivo rispetto a un'istantanea, e fa riferimento ai Regolamenti (*Covenant*) dei terreni.

In particolare, in base alle nuove disposizioni è sempre possibile fotografare una land e i suoi contenuti, a meno che sia vietato dallo specifico Regolamento di quella *land*.

Di conseguenza, data l'assenza di *Covenant*, in *Mainland* è sempre permesso fotografare.

Non serve alcun permesso per fotografare altri *avatar*.

È invece sempre necessario il permesso degli utenti che vengono filmati, a meno che siano di fatto irriconoscibili (per l'assenza del nome, l'uso di un personaggio sufficientemente generico e/o le ridotte dimensioni).

Per filmare una *land* e i suoi contenuti, è sempre necessario il permesso esplicito dei proprietari della *parcel*. Nelle regioni private il proprietario può concedere *a priori* il permesso di girare video nella sim, scrivendolo nel Regolamento.

A prescindere da quello che dicono o non dicono i Regolamenti / *Covenant*, è sempre possibile contattare i proprietari delle singole *parcel* per ottenere i permessi necessari.

La *Snapshot and Machinima Policy* non impone di richiedere permessi ai creatori degli oggetti presenti in immagini e filmati, fatto salvo il caso di eventuali *trademark* – che generalmente non esistono per i prodotti in commercio.

Fatto salvo il rispetto dei Regolamenti dei terreni e della volontà degli utenti nel caso dei video, la nuova *policy* consente di fotografare e filmare tutto quello che è visibile all'interno di *Second Life*, e di riutilizzare in qualsiasi modo le *snapshot* e i *machinima* così creati.

Come sempre, vanno inoltre presi in considerazione sia i principi del *fair use* della legislazione statunitense, sia le norme generali del diritto d'autore, sia tutte le altre regolamentazioni del servizio indicate da *Linden Labs*.

13. Conclusioni

La regolamentazione di *Second Life*, e più in generale del *web*, dovrebbe quindi forse essere affidata ad una carta dei diritti valida ovunque e per chiunque?

Ma un *Internet Bill of Rights,* per la natura stessa dell'oggetto su cui incide, dovrebbe piuttosto essere il frutto di un approccio pluralista e democratico con tutte le componenti coinvolte a fungere da attori protagonisti. Non sarebbe, in questa ottica, neppure corretto adottare le classiche procedure delle convenzioni internazionali, attraverso forme di cooperazione tra governi che potrebbero produrre un testo da sottoporre poi, ad esempio, all'approvazione all'Assemblea generale delle Nazioni Unite.

Ciò potrebbe piuttosto costituire l'atto conclusivo, finale di una procedura comunque *multilevel* e *multistakeholders*.

Così al *Dialogue Forum on Internet Rights*, svoltosi a Roma nel settembre 2007, è stata proposta una "Costituzione di Internet", con lo scopo di creare uno statuto di autogoverno al fine di impedire regolamentazioni esterne, siano esse ottriate o approvate da assemblee costituenti, e ciò, per dirla con le parole di Stefano Rodotà, "in quanto la natura stessa di Internet si oppone all'adozione di questo schema". Internet è infatti il luogo del dialogo esteso che mira all'elaborazione comune in un'ottica, richiamata dai migliori commentatori, di *multistakeholders*[31].

La Carta per Internet non può che essere il risultato di un processo iniziato ad Atene nel 2006 con il primo *Internet Governance Forum*, ove si sono materializzate alcune "coalizioni dinamiche"[32], gruppi interessati alla preparazione di un documento da inserire su Internet e sul quale aprire una discussione globale.

Va posta anzitutto la questione di una politica complessiva di gestione della cosiddetta *net neutrality*, ossia l'indipendenza della struttura di rete

[31] Con tale termine deve intendersi la partecipazione di una molteplicità di soggetti rappresentativi di una varietà di culture, interessi, aree geografiche.

[32] Le coalizioni dinamiche rappresentano un nuovo soggetto diffuso e pluralista, costituito spontaneamente dall'aggregazione di singoli e gruppi; esse possono diventare le protagoniste del processo istitutivo dell'*Internet Bill of Rights*. Cfr. sul punto S. Rodotà, *Towards an Internet Bill of Rights*, paper al "Dialogue Forum on Internet Rights", Roma, 27 settembre 2007, reperibile all'url http://www.dfiritaly2007.it/pdf/Intervento_Rodota.pdf.

rispetto alla tipologia dei dati e contenuti da essa trasmessi. È un tema, questo, che ha ripercussioni sulla natura stessa della rete e delle sue modalità di gestione e che oggi assume particolare rilevanza, posto che essa costituisce un prerequisito, non solo tecnico, nei confronti del riconoscimento del diritto di accesso alle nuove tecnologie in un'ottica di uguaglianza sostanziale.

Accanto a ciò, c'è poi l'esigenza di riconoscere la libertà di espressione, di circolazione e fruizione dei contenuti di una rete che è divenuta sempre più capace di "creare dal basso", a partire cioè dalle capacità e potenzialità degli stessi utenti, tenendo però conto delle esigenze di protezione dei dati personali, tutela dei diritti dei minori, salvaguardia delle categorie vulnerabili, e rispetto della diversità culturale[33].

Bastano questi esempi per evidenziare che la *governance* dello sviluppo della rete ha dimensioni evidentemente diverse da quella dei tradizionali ambiti delle politiche nazionali.

Di ciò si ha riprova osservando le procedure di riassegnazione dei nomi a dominio, che trovano valida base nell'autonomia contrattuale, in una sorta di autogoverno dei consociati, così descritte all'interno delle regole di *naming*[34].

Contestualmente all'elaborazione dei contenuti di una Carta dei diritti di Internet, è necessario individuare gli strumenti idonei a garantire che tali valori siano realmente accreditati come riferimento per gli individui, i gruppi, le imprese o gli Stati, affinché lo sviluppo della "società dell'informazione" sia davvero incentrato sul rispetto e la promozione di diritti universalmente riconosciuti.

Così alcuni[35] propendono per un significativo rafforzamento del ruolo delle Nazioni Unite, non con funzioni repressive, ma con il fine ultimo di rafforzare il legame tra lo sviluppo della rete ed il rispetto di diritti universali.

[33] L. NICOLAIS, *Intervento* al "Dialogue Forum on Internet Rights" (Roma, 27 settembre 2007), reperibile all'url http://www.dfiritaly2007.it/pdf/Intervento_Nicolais.pdf.

[34] Le regole di *naming* costituiscono il contenuto pattizio del contratto che è alla base dell'attività del Registro di assegnazione dei nomi a dominio. È appena il caso di sottolineare come le procedure di riassegnazione non abbiano carattere giurisdizionale e consentano comunque alle parti il ricorso alla magistratura.

[35] L. NICOLAIS, *op. cit.*

Ripercorrendo le funzioni delle Nazioni Unite che hanno visto tale organismo come referente collettivo per altri temi di carattere universale, quali l'ambiente o gli stessi diritti umani, anche per Internet potrebbe, per alcuni, costituirsi una figura di "Alto Garante" dei diritti della rete che, a partire da un ampio mandato e sostegno internazionale, sia in grado di costituire consenso e facilitare il processo di elaborazione dei diritti fondamentali di Internet, ma anche, in futuro, farsi portavoce dell'adozione del rispetto di quei diritti.

Viaggio nei metaversi alla ricerca del diritto perduto

MARIA CONCETTA DE VIVO*

1. I MONDI VIRTUALI. NATURA E PROBLEMATICHE

Internet assomiglia sempre più ad un organismo vivente e come tale è naturalmente destinato a crescere e modificarsi.

Lo stesso *web 2.0* si sta evolvendo inevitabilmente in forme sempre più sofisticate e interattive. Si sta approdando a una tipologia di rete in cui i soggetti coinvolti sono passati da semplici fruitori a creatori di contenuti e ciò fa riflettere su quanto sia veloce l'evoluzione di questo mondo tecnologico che non rispetta i lenti parametri temporali dell'uomo.

All'ambiente *web* (considerato come una forma ormai datata di interazione in rete) subentrano i *social network* che permettono all'individuo di condividere vita, passioni, attività lavorative con milioni di altre persone presenti in Internet. Si moltiplicano le identità virtuali all'interno di Internet e spesso accade che ogni individuo sia titolare di molteplici cyberidentità[1].

All'era del *blogging* si affianca quella del *tagging*, attività nota ai frequentatori di Facebook e di altri *social network* simili, in cui ogni oggetto (evento/immagine) viene taggato, segnalato, commentato e poi "sparato" in rete per la solita, inevitabile e a volte inutile, necessità di condivisione.

Applicativi come Google latitude[2] permettono, a chi ne è in possesso sul proprio telefonino o sul proprio palmare, di rintracciare amici, mogli

* L'Autrice è ricercatrice confermata di Diritto privato presso l'Università di Camerino, è docente di Diritto dell'informatica e di Diritto dell'economia e dell'amministrazione digitale presso la Facoltà di Giurisprudenza e di Diritto delle nuove tecnologie presso la Facoltà di Scienze e tecnologie della stessa Università. È autrice di saggi dedicati al diritto e nuove tecnologie.

[1] Si stanno studiando applicativi in grado di monitorare e informarsi sia sulle persone sia sui rispettivi *alter ego* digitali.

[2] http://www.google.it/latitude/intro.html. Nella pagina su Google latitude si legge che "è una funzione di Google Maps per cellulari supportata sui seguenti dispositivi: dispositivi

o mariti, considerati come contatti, e invitarli a condividere la propria posizione geografica. Il servizio è attivabile e disattivabile su richiesta, si può accedere attraverso *login* ed è possibile utilizzarlo solo dopo aver ottenuto l'autorizzazione del "contatto". Nell'autorizzazione l'utente potrà decidere cosa permettere di vedere e le modalità di un eventuale monitoraggio. Una volta identificata la posizione del contatto si potrà interagire con questo telefonicamente, per sms o per *chat*.

Google latitude è già a disposizione in ben 27 Paesi nel mondo (Italia compresa), ha al suo attivo 8 milioni di utenti registrati di cui 3 milioni attivi[3] ed è considerato una forma di geolocalizzazione in chiave sociale.

La pubblicità dell'applicativo è sconcertante. Nella home page di presentazione, tra gli *spot* del prodotto, si legge: "Controlla lo stato dei tuoi amici per scoprire cosa stanno facendo" oppure " Mia moglie sta rientrando dal lavoro … è meglio che cominci a preparare la cena". Ciò che lascia perplessi non è il costante attentato alla *privacy*, che è fatta salva dal classico meccanismo di accettazione della condivisione da parte dell'utente[4], bensì il desiderio, avvertito da milioni di persone, di voler condividere ogni-cosa-sempre-e-subito con il maggior numero di individui, pretendendo, nonostante tutto, di conservare intatta la propria sfera privata.

Internet diventa *mobile* e sempre più pervasiva per la sua stessa facilità di fruizione.

In questo scenario i mondi virtuali rappresentano una evoluzione della "nuova" tecnologia; tendono ad affiancarsi sempre più spesso e sempre più facilmente al mondo reale, a volte sovrapponendosi ad esso, fino a diventare pericolosamente sostitutivi della stessa realtà[5].

dotati di piattaforma Android, ad esempio T-Mobile G1; dispositivi iPhone e iPod con *touch-screen* (in arrivo); la maggior parte dei dispositivi BlackBerry; la maggior parte dei dispositivi basati su Windows Mobile 5.0 e versioni successive; la maggior parte dei dispositivi basati su Symbian S60 (smartphone Nokia)".

[3] Dati estrapolati da Motori di Ricerca del 7 maggio 2010, http://www.motoricerca.net/2010/05/07/google-latitude-checkin.

[4] Nel pannello di controllo di Latitude si ha immediatamente accesso ad opzioni che permettono di gestire la propria *privacy*.

[5] Questo a causa della costante e facile interconnessione tra virtuale e reale attraverso l'uso di palmari o cellulari di ultima generazione.

Il proliferare dei metaversi[6] denota la propensione, da parte del singolo individuo, per una nuova forma di comunità basata sul concetto di "rete".

È evidente che i mondi virtuali sono, come le comunità "reali", luoghi in cui i soggetti interagiscono fra di loro, riproducendo un complesso sistema sia sociale sia economico e conservando al contempo la loro originaria natura di "formidabile mezzo di comunicazione in tre dimensioni". Diventa, dunque, necessario coglierne gli aspetti particolari, capirne la vera natura e tentare un approccio giuridico volto a regolarizzare le attività umane che in essi si svolgono.

In questi metaversi, gli individui si organizzano, lavorano, studiano e spesso svolgono transazioni[7], guadagnando e investendo; sostanzialmente socializzano, come accade nella vita reale. Non si capisce, dunque, per quale motivo tutte queste attività umane debbano sfuggire al "controllo" e ai mezzi di tutela approntati dal diritto nella quotidiana realtà.

Le problematiche giuridiche legate all'assenza di uno Stato, alla aterritorialità, alla deresponsabilizzazione, tipiche del mondo di Internet, si ripropongono anche nei metaversi.

A volte è possibile applicare il diritto positivo in questi mondi digitali, come nel caso in cui si verificano illeciti penali. Si pensi alla pedopornografia, al vandalismo contro gli oggetti di proprietà degli utenti, alla violazione di domicilio (informatico), alla violazione del diritto d'autore, all'abuso e contraffazione di marchio, ai casi di ingiuria e/o diffamazione e infine all'abuso e furto di identità. Le problematiche inerenti l'ambito privatistico, come quelle legate ad attività lavorative o commerciali *on line*,

[6] Il termine "metaverso" indica una realtà virtuale in cui è possibile vivere grazie ad un proprio avatar in 3D ed è ripreso dalla fantascienza cyberpunk, così come molti altri termini che riguardano Internet. Il metaverso, così come è ormai comunemente inteso oggi, è immaginato per la prima volta nel libro "Snow Crash" di Neal Stephenson pubblicato nell'ormai lontano 1992, un vero e proprio tecno-giallo. Già in precedenza un altro autore, altrettanto noto nell'ambiente cyberpunk, William Gibson, aveva parlato di cyberspazio. Incredibilmente Neal Stephenson nel suo libro ha previsto, con molti anni di anticipo, il mondo virtuale di *Second Life*, raccontando le peripezie del protagonista, l'ultimo *hacker free lance* Hiroaki "Hiro" Protagonist.

[7] Attraverso semplici acquisti del tipo C2C oppure attuando forme complesse di commercio elettronico.

sono le più difficili da regolamentare, mentre restano confinate nel fanta-diritto alcune ipotesi decisamente speciali, come ad esempio quelle legate alla figura dell'avatar, e la difficoltà di individuare il suo ruolo nell'effimero mondo virtuale[8].

I metaversi suscitano interesse anche da un punto di vista medico-legale. Se da un lato l'analisi del rapporto tra individuo e il proprio avatar può portare ad evidenziare vere e proprie forme di dipendenza da *web* e da MMORPG[9], dall'altro lato appare evidente il legame che può instaurarsi tra un soggetto diversamente abile e il proprio avatar. Per il soggetto diversamente dotato a volte l'*alter ego* digitale può rappresentare una sorta di prolungamento della propria fisicità, uno strumento particolarmente adeguato a svolgere attività e funzioni che altrimenti gli sarebbero preclusi, permettendogli di accedere all'interno della comunità virtuale con particolare facilità, sicuramente maggiore rispetto al suo inserimento nel mondo reale.

Tutto ciò porta a chiedersi che natura abbiano i metaversi, se, cioè debbano intendersi come "semplici" strumenti di gioco oppure come strumenti di comunicazione e di interazione sociale dai quali i soggetti a rischio (disabili e minori) debbono essere particolarmente tutelati.

Pur volendo minimizzare l'impatto che i metaversi hanno nella realtà, per la loro originaria natura ludica, è bene ricordare che il gioco è comunque una forma primordiale di attività formativa. *Second Life* (SL) e gli altri metamondi, appaiono sempre più simili a *serious games*, ossia a giochi ideati non solo per insegnare e imparare ma anche per sperimentare nuove forme di attività aziendali, per scopi medico-terapeutici, per effettuare sondaggi, per svolgere particolari forme di comunicazione (ad esempio politica) e così via; diventano, cioè, ambienti (virtuali) in cui le aziende provano "nuove idee su scala ridotta"[10] al fine di testare strategie promozionali.

[8] Solo quando l'avatar non è utilizzato per giocare ci si accorge della sua funzione di rappresentare e identificare l'individuo all'interno di una vera e propria comunità, pur se virtuale.

[9] Massively multiplayer online role-playing game. Sostanzialmente un gioco di ruolo di ultima generazione.

[10] Così in una intervista di Henry Jenkins, per 16 anni docente al Massachusetts Institute of Technology (MIT), apparsa su www.2litaliaworld.it/pdfrivista/2L_4.pdf.

È ormai diffuso l'utilizzo di questi strumenti in 3D per scopi di formazione a distanza e di studio, dove la presenza di avatar e la riproduzione di ambienti realistici contribuiscono ad "umanizzare" il *software* e l'ambiente informatico in genere. Molte sono le Università in SL[11] e con la loro presenza hanno dato vita ad una nuova forma di *e-learning*.

La natura informatica dei metaversi pone, inoltre, problematiche legate alla gestione e al corretto funzionamento della piattaforma e del *software* utilizzati per creare e gestire una società virtuale, ma soprattutto alle relative responsabilità per i possibili danni causati dal *software*.

2. L'identità personale nei metaversi. Il caso *Second Life*. L'avatar

La tecnologia influenza pesantemente l'organizzazione umana e di conseguenza, più o meno direttamente, il diritto, ossia le norme adottate per regolare i rapporti interpersonali che sorgono all'interno di una *societas*.

Sorvolando sul fenomeno dei *social networks*, l'altra faccia della rete che desta curiosità è quella dei "mondi virtuali". L'argomento è oggetto di studio soprattutto da parte di sociologi ed esperti di comunicazione[12].

Si è affermato da più parti che l'uomo "è naturalmente predisposto ad agire tecnologicamente". La tecnologia può intendersi come un rafforzamento delle potenzialità umane[13], perso con l'avvento della tecnologia delle macchine che ha interrotto l'effetto antropocentrico dei processi tecnologici: "L'opera della costruzione delle macchine è elevata espressione della capacità umana di riplasmare il dato a misura d'uomo [...] e nel contempo, proprio con questa creazione, viene messa al mondo una nuova entità, un nuovo processo che, in modo definitivo e prima inim-

[11] Soprattutto negli Stati Uniti, molto meno in Italia

[12] Un convegno internazionale svoltosi nel 2009 presso l'Università di Urbino ha visto la partecipazione dei maggiori esperti di *social network*. Il materiale della nona conferenza mondiale di sociocibernetica tenutasi dal 29 giugno al 5 luglio ad Urbino, dal titolo *Modernity 2.0 a Urbino con danah boyd* è reperibile in http://larica.uniurb.it/nextmedia/2009/05/modernity-20-a-urbino-con-danah-boyd/

[13] Così come è accaduto per l'uomo primitivo con la creazione della lancia, all'epoca uno strumento tecnologico d'avanguardia che, di fatto, ha reso più facile la caccia potenziandone l'esito positivo (H. Popitz, *Verso una società artificiale*, Roma, Editori Riuniti, 1996).

maginabile, espone l'uomo a una eterodeterminazione per mezzo di ciò che ha creato"[14]. In questo contesto la tecnologia deve essere considerata "non come strumentale all'evoluzione umana, ma come sostanziale (…), la storia della tecnica è storia dell'uomo stesso e della sua cultura e, contemporaneamente, è espressione di una connaturata predisposizione ad agire, perseguendo lo scopo di razionalizzare il mondo e la propria posizione in esso, anche producendo ciò che in natura non è dato: l'artefatto (…) l'agire tecnico è intimamente legato all'organizzazione sociale ed economica e alla rappresentazione che un determinato gruppo umano ha di sé stesso"[15].

I metaversi sono l'aspetto più entusiasmante della "nuova" tecnologia e perciò devono necessariamente confrontarsi con l'uomo e con le regole che questo si è dato.

In simili contesti ci si chiede che interesse può avere un mondo virtuale per il diritto e per il giurista.

Se il fenomeno fa riferimento ai MMORPG e resta limitato nell'ambito del gioco, il problema non si pone a meno che non si debbano affrontare le problematiche connesse alla liceità del gioco stesso. Ma spesso questi mondi virtuali non sono solo gioco, perché riproducono sistemi economici e sociali, strutture complesse con soggetti che, sotto forma di avatar, si aggregano, dando vita a vere e proprie formazioni sociali.

È bene ricordare, sempre e comunque, che Internet e tutti i fenomeni ad essa connessi, come i *social network*, i *blog*, i siti *web* di prima, seconda e ultima generazione e gli stessi mondi virtuali, sono innanzitutto potenti mezzi di comunicazione e che il loro utilizzo deve essere regolamentato perché sono naturalmente predisposti a trasformarsi, da strumenti utili e geniali, in strumenti estremamente pericolosi per l' utente.

Tuttavia, parlare di "regolamentazione giuridica" di Internet è (ancora) impopolare e controproducente C'è il rischio d'essere fraintesi e d'essere scambiati per reazionari e pericolosi censori di vecchia generazione, ma non è così. Tutto ciò che riguarda i rapporti interpersonali deve rien-

[14] H. POPITZ, *op.cit.*, p. 23.

[15] A. SPINELLI, *La tecnologia: nature artificielle dell'umano*, in "Dialegesthai. Rivista telematica di filosofia", 2008, in http://mondodomani.org/dialegesthai/as02.htm.

trare nello schema delle regole di una società civile, formata da individui titolari di diritti e di doveri, qualunque sia il contesto in cui questi rapporti si instaurano. Nell'ipotesi dei metaversi, la difficoltà sta nel richiedere all'operatore del diritto uno sforzo rilevante di interpretazione per contestualizzare correttamente le norme giuridiche nel nuovo ambiente; questo però non autorizza a pensare che Internet possa sfuggire al diritto.

Quotidianamente si hanno notizie sulla disinformazione attuata attraverso *web* o *blog*, su nuove forme di violazione della *privacy* attraverso l'utilizzo (scorretto) dei *social networks*; su casi di spamming di ogni tipo e sulla crescente difficoltà di poter effettuare in (relativa) sicurezza i propri acquisti *on line*. Tutto ciò vanifica la portata rivoluzionaria di Internet intesa come straordinario strumento tecnologico in grado di agevolare la vita sociale del cittadino-utente-e-consumatore e ripropone l'esigenza di creare regole giuridiche anche nelle c.dd. comunità virtuali.

Alcuni di questi metaversi riproducono la vita reale con peculiarità e differenze minime e la *slogosphere*[16] si popola di ambienti che hanno solo l'apparenza di giochi. Tra i più conosciuti "universi sintetici *on line*", oltre SL, ci sono:

- Entropia[17],
- World of Warcraft[18],

[16] Tipico esempio è l'ambiente di *Second Life*.

[17] www.entropiauniverse.com. Entropia Universe è stata fra le prime realtà digitali a privilegiare l'aspetto economico del gioco, basando la propria comunicazione sulle possibilità di arricchimento dei partecipanti. Questo metaverso è stato creato da una società svedese nel 2004. Il giornalista Mario Gerosa, esperto di questi fenomeni, su Entropia ha affermato, in una intervista, che "È già un mondo trendy, anche se l'attenzione all'immagine non è sviluppata come in *Second Life* (…). Il mondo non è creato dai giocatori, che, invece, sono impegnati in attività ludiche come la caccia o la lotta. Ci si può addentrare in angoli simili alle cittadine medievali inglesi, in cittadelle sovietiche o in regni del divertimento come la Treasure Island che è stata al centro della prima grande transazione di un bene virtuale".

[18] www.worldofwarcraft.com. In World of Warcraft si vive in una atmosfera *fantasy*. "Anche in Wow esiste un'infrastruttura economica, ma non ha nulla a che fare con quella del mondo reale, come accade invece in *Second Life* o Entropia (…). Qui il vero miracolo economico lo hanno fatto i gestori della Blizzard, che hanno creato un modello di business invidiabile, che ha addirittura gemmato una vera e propria letteratura tradotta in più lingue. La grafica è molto più dettagliata che negli altri due mondi e i legami che si creano tra i giocatori molto profondi. Spesso si organizzano in gruppi (gilde) per portare a termine le missioni che i demiurghi della

- Farmeville[19] e
- HipiHi[20].

In tutti questi ambienti il principale problema giuridico è quello connesso all'identità personale. L'avatar è il mediatore che permette all'individuo in carne e ossa di interagire con il mondo digitale in cui viene proiettato, ed è su questa figura che si concentra l'attenzione del giurista per valutare se possa considerarsi come una nuova espressione di identità personale.

Il concetto di identità può essere analizzato sia sotto l'aspetto filosofico sia giuridico.

L'identità[21], da un punto di vista filosofico, potrebbe semplicisticamente essere riassunta come "la coscienza di sé". Per coscienza di sé si intende "la volontà-la coscienza-la memoria" delle proprie azioni. L'identità di

Blizzard assegnano. Più che di architetture, in questo caso (…) si tratta delle scenografie di un nuovo genere di entertainment che ha qualcosa a che vedere con il cinema". Così parla di World of Warcraft F. Todesco in una breve notizia apparsa nel 2007, *Viaggio ai confini del metaverso*, in www.viasarfatti25.unibocconi.it/notizia.php?idArt=587, riportando a sua volta stralci di interviste con Matteo Esposito, altro esperto dei metaversi dell'agenzia di comunicazione Imille.

[19] Il gioco on line di Farmville nasce sull'onda della "moda" lanciata dalla *first lady* americana Michelle Obama. Consiste nel creare dal nulla una fattoria e imparare a gestirla proprio come farebbe un imprenditore agricolo in carne e ossa. Per partecipare a questo gioco di ruolo sono richieste disciplina, creatività e l'impegno a realizzare una strategia vincente. Il protagonosita è un avatar-agricoltore che deve far produrre la propria fattoria virtuale attraverso scelte e decisioni da imprenditore agricolo, come ad esempio l'opportunità di effettuare investimenti nelle piantagioni. Le regole del gioco consistono nell'assegnazione di sei unità di terreno coltivabile e un budget iniziale. Rendere coltivabile un'area e piantarci frutta e verdura ha un costo, che varia da coltivazione a coltivazione. Lo scopo è espandersi e aumentare i punti in modo da poter salire di livello, e più si sale più aumentano le possibilità di investimento e di abbellimento della fattoria. Sul nuovo fenomeno che spopola su Facebook sono stati scritti già numerosi articoli, l'ultimo in ordine di tempo è quello pubblicato su La Stampa del 12 ottobre 2009 www.lastampa.it/_*web*/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=6746&ID_sezione=38&sezione=News).

[20] www.hipihi.com. La versione cinese di SL, ideata nel 2007 ma che trova difficoltà a decollare nonostante alcune novità determinanti che rendono la vita agli avatar più facile che in SL.

[21] Sulla identità personale per una bibliografia giuridica di base di riferimento e di approfondimento: D. MESSINETTI, voce *Personalità (diritti della)*, in "Enciclopedia del Diritto", XXXIII, 1983, pp. 371 e ss.; P. PERLINGIERI, *La personalità umana nell'ordinamento giuridico*, Napoli, ESI, 1972; A. BALDASSARRE, *Diritti della persona e valori costituzionali*, Torino, Giappichelli, 1997; P. RESCIGNO, *Personalità (diritti della)*, in "Enciclopedia del Diritto", XXIV, 1990.

una persona può fare riferimento sia all'aspetto soggettivo interiore (il c.d. "io") sia alla vita di relazione che quell'"io" svolge all'interno di una comunità (c.d. "io sociale"). In tal caso la manifestazione dell'io avviene in due forme: una identità individuale, con riferimento all' "individuo", e una identità relazionale, con riferimento alla "vita di relazione" che quell'individuo svolge in quanto essere pensante.

Il diritto coglie questi due aspetti della identità personale, tutelando sia l'individuo e la sua esigenza di vedersi riconosciuto in quanto tale dagli altri consociati, sia le azioni che "quel" determinato individuo pone in essere in quanto partecipe di una comunità, tutelando, sostanzialmente, la sua vita sociale.

In dottrina l'espressione "identità personale" è stata elaborata, in modo articolato, da De Cupis[22].

In giurisprudenza termine e concetto furono analizzati e richiamati per la prima volta da una storica sentenza della Cassazione[23] del 1985. In realtà già una decisione del 1974 fece da *case study*[24] riconoscendo accanto ai già noti diritto al nome e all'immagine un ulteriore, e all'epoca semisconosciuto, "diritto all'identità personale".

Nella ricca produzione giurisprudenziale che seguì si prese atto che il soggetto "(sia esso, indifferentemente, persona fisica, persona giuridica, entità associativa non personificata, ma rilevante per l'ordinamento) nella

[22] Tale autore identifica l'interesse all'identità personale nella "volontà del soggetto di essere rappresentato nella sua reale essenza attraverso la tutela al diritto dell'uso esclusivo di certi segni distintivi (nome, pseudonimo) in modo da escludere confusione con gli altri consociati ed esercitando in caso, l'azione di usurpazione", A. DE CUPIS, *I diritti della personalità*, Milano, 1982, pp. 541 e ss. Tuttavia si hanno già delle prime elaborazioni nella metà del '900.

[23] "Nell'ordinamento italiano sussiste, in quanto riconducibile all'art. 2 Cost. e deducibile, per analogia, dalla disciplina prevista per il diritto al nome, il diritto all'identità personale, quale interesse, giuridicamente meritevole di tutela, a non veder travisato o alterato all'esterno il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale ecc. (nella specie: dal testo di un'intervista resa ad un settimanale dal direttore dell'istituto tumori di Milano, era stata estrapolata, per poi esser riprodotta in un inserto di pubblicità redazionale, un'affermazione circa la minor nocività di sigarette leggere; sulla base del principio dianzi riportato, è stata confermata la condanna generica di risarcimento del danno a carico della società produttrice delle sigarette reclamizzate, nonché dell'agenzia pubblicitaria)", Cass., 22 giugno 1985, n. 3769, "Foro italiano", 1985, I, c. 2211.

[24] Pret. Roma, 6 maggio 1974, in "Giurisprudenza italiana", 1975, 2, pp. 514 e ss.

sua proiezione politica e sociale assume una peculiare connotazione, una specifica identità ideologica, ponendosi come titolare di un patrimonio di idee, e che va tutelato contro eventuali rappresentazioni difformi, suscettibili di stravolgere l'acquisita identità"[25].

Il diritto considera l'identità personale sotto un duplice aspetto: a) in riferimento al complesso quadro di informazioni anagrafiche volte ad identificare l'individuo nella sua vita di relazione con la pubblica amministrazione, oppure b) riconoscendo tutti quei dati che fanno parte della "storia" dell'individuo stesso e che sono in grado di contraddistinguerlo dagli altri consociati.

La persona, nella sua globalità, è tutelata da una serie di disposizioni normative contenute sia nella nostra Costituzione (artt. 2 e 22) sia in altri testi come, ad esempio, il Codice civile (artt. 6, 7, 8, 10 e 2575), il Codice penale (artt. 594 ss.), la legge sul diritto d'autore (artt. 20, 96 e 97), la legge sulla stampa (art. 8)[26] e la legge sulla *privacy*.

L'identità personale si pone, nei confronti di questa frammentata serie di disposizione normative, come un diritto che integra e completa, di volta in volta, le varie sfaccettature della tutela della persona, alla luce della fondamentale disposizione costituzionale (art. 2).

Alcune sostanziali differenze si notano:

a) tra diritto all'identità personale e diritto all'immagine. Nel diritto all'immagine, ad esempio, si fa riferimento ad un elemento "materialmente percepibile e riproducibile" mentre il diritto all'identità personale si riallaccia ad aspetti più squisitamente "morali" o comunque "spirituali" della personalità;

b) con il diritto alla riservatezza che tende a realizzare il desiderio del soggetto a che le proprie vicende private restino tali e quindi siano protette dalla conoscenza (o curiosità) da parte di altri. Nell'identità personale, invece, ciò che si vuole realizzare è la "massima chiarezza possibile" circa il complesso di attività che rilevano la connotazione della propria personalità[27]. I due aspetti sembrano, tuttavia, convergere e coincidere, laddove si fa riferimento alla raccolta e trattamento delle informazioni sull'indivi-

[25] Cfr. V. ZENO ZENCOVICH, *Identità personale*, in "Digesto", Utet, 1993, p. 10.

[26] Laddove viene disciplinato il diritto di rettifica, a prescindere dalla tutela della reputazione e con riferimento ad una più generica e onnicomprensiva tutela della identità personale.

[27] V. ZENO ZENCOVICH, *op. cit.*, pp. 17 e ss.

duo da parte di strumenti informatici. In questo caso la tutela dall'altrui intrusione in fatti e comportamenti privati (diritto alla riservatezza) si arricchisce e si completa con una ulteriore protezione (diritto all'identità personale) consistente nel riconoscere al soggetto una tutela in grado di inibire qualsiasi forma di raccolta di dati[28] da parte di altri sulla propria identità, che impedisca all'interessato di disporne in modo esclusivo;

c) con il diritto morale d'autore, che sembra rappresentare una forma di identità personale circoscritta alla personalità dell'autore. È, infatti, "evidente come il diritto alla paternità dell'opera, allo pseudonimo, al ritiro dal commercio, costituiscono forme di tutela delle manifestazioni esterne del carattere dell'artista: il soggetto esercitando tali diritti chiede che lo si riconosca per quel che è e per quello che ha fatto"[29];

d) altre sostanziali differenze si riscontrano tra l'identità personale e la reputazione. La più eclatante consiste nel fatto che mentre la prima riguarda la conoscenza che la collettività ha della persona, la seconda è espressione di un giudizio che la collettività dà sulla persona.

L'articolo 2 della Costituzione sostanzialmente riconosce nell'identità personale il diritto "ad essere sé stesso" intendendo come "sé stesso" sia il soggetto (la persona in sé) sia la sua vita associata, ossia le proprie idee, esperienze e convinzioni. Un diritto che consiste, dunque, nel vedersi riconoscere "la paternità delle proprie azioni", ciò a significare la unicità del soggetto inteso sia come corpo, o immagine di sé, sia come attività, o come manifestazione della sua volontà di esistere. Una sorta di "formula sintetica per contraddistinguere il soggetto da un punto di vista globale nella molteplicità delle sue specifiche caratteristiche e manifestazioni"[30].

Il concetto di identità personale appare, dunque, strettamente connesso con quelli di comunità, gruppo, società e "mondo" inteso, quest'ultimo, come ambiente (reale o virtuale che sia) popolato da un insieme di individui che in esso vivono e si contraddistinguono.

La comunità sociale virtuale è un "luogo" come qualsiasi altro in cui il soggetto decide di relazionarsi con gli altri consociati e dove, perciò, ogni sua attività e manifestazione necessita di adeguata tutela.

[28] Non necessariamente privati.

[29] V. ZENO ZENCOVICH, *op. cit.*, p. 17.

[30] D. MESSINETTI, *op. cit.*, p. 371.

Sono molti gli aspetti che debbono essere regolamentati giuridicamente anche negli ambienti virtuali e sono tutti la conseguenza logica del fatto che l'individuo decide di svolgervi una qualsiasi attività.

In una comunità virtuale le veci della "corporalità" vengono espletate da un surrogato adeguato all'ambiente digitale, per cui sia l'identità individuale, intesa come immagine dell'individuo, sia l' identità sociale, intesa come la sua capacità d'essere riconosciuto e di relazionarsi con gli altri, vengono soddisfatte da un avatar, ossia da una identità digitale che permette all'individuo di agire nella sua vita sociale in rete.

L'avatar[31] diventa, dunque, una proiezione e una manifestazione di sé stessi e la sua natura incorporea permette al soggetto di esprimersi in assoluta libertà. Molti avatar non si limitano ad una semplice riproduzione speculare dell'individuo e così accanto a doppi antropomorfi si affiancano altri, zoomorfi o fantastici.

Alcuni giocatori, intervistati sui propri avatar, hanno ammesso di essersi ispirati, nella creazione del proprio *alter ego*, più che al proprio aspetto fisico, a ciò che interiormente sentono di sé stessi e che quindi vogliono "comunicare" agli altri. È il caso di chi si rappresenta come un cavaliere medioevale perché crede fortemente nei valori di lealtà, amicizia, sincerità e generosità che sono valori tipicamente cavallereschi, oppure persone che scelgono d'essere rappresentati da un avatar provvisto di ali perché vogliono esprimere la leggerezza dell'essere o la propria disponibilità ad aiutare i nuovi arrivati.

Strettamente collegato all'avatar è il discorso sulla riconoscibilità dell'individuo o sul suo diritto a restare anonimo.

Gli avatar con cui si opera nei mondi digitali sono immeditamente identificabili perché dotati di una etichetta che li sovrasta e che permette a chiunque di riconoscere ogni singolo personaggio e contattarlo. Il problema è che proprio per questa sua facile identificabilità, può essere oggetto di vere e proprie forme di *spamming* e altre molestie.

[31] È ormai a tutti nota l'etimologia della parola che deriva dalla lingua sanscrita e significa "disceso". Nella religione induista sta ad indicare l'incarnazione di un Deva, ossia di una divinità, in un corpo fisico al fine di svolgere determinati compiti. Nei metaversi, l'avatar sta ad indicare la possibilità dell'individuo di fare cose che solo una divinità potrebbe fare, come volare, non morire mai, non provare dolore e trasportarsi ovunque.

Il fatto che in *Second Life* e nei metaversi in genere esista una netiquette che deve essere rispettata da tutti gli avatar, non mette al sicuro da forme di violazioni (o di "semplice" disturbo) della propria *privacy*[32]. Il discorso si allarga fino a ricomprendere tutta una serie di problematiche legate alla tracciabilità e al monitoraggio del soggetto e all'uso dei dati raccolti su di lui per fini commerciali. In *Second Life* ci sono molte "società" che investono tempo e denaro per monitorare il traffico in rete e sapere chi c'è *on line* e cosa fa.

L'avatar, tecnicamente parlando, è il prodotto di un *software* che, in determinate ipotesi, può svilupparsi in forme di intelligenza artificiale. È il caso dell'esperimento effettuato dal Dipartimento di Scienze cognitive dell'Istituto Politecnico di Renssealer che ha creato un bimbo-avatar dal nome Eddie.

Eddie è il risultato di una particolare architettura di intelligenza artificiale "che ha proprie convinzioni ed è capace di ragionarci sopra per arrivare a delle conclusioni con dinamiche paragonabili a quelle dei bambini reali di quattro anni"[33]. L'intento che ha mosso l'esperimento è la previsione dei comportamenti attraverso la simulazione e lo studio delle condotte umane in casi estremi (come ad esempio nell'ipotesi di attacco terroristico). Sostanzialmente questa nuova forma di "ingegnerizzazione" avrebbe lo scopo di permettere ad agenti intelligenti (*software* particolarmente sofisticati travestiti, in questo caso, da avatar) di riprodurre il comportamento umano, di capire, prevedere e dunque manipolare altri agenti e fornire, con relativa attendibilità, risposte e sviluppi a scenari inquietanti.

L'avatar, inoltre, può rappresentare uno straordinario prolungamento del proprio corpo, utile soprattutto per determinate categorie di soggetti, come i diversamente abili. È il caso del non vedente che decide di entrare in un metamondo e che, esattamente come avviene nel mondo reale, ha bisogno di un supporto che gli permetta di muoversi nell'ambiente digitale che lo circonda. L'Accessibility in Virtual Worlds dell'IBM è un *tool* in grado di descrivere l'ambiente circostante, integrato "da sistemi di sintesi vocale

[32] V. sull'argomento E. BERLINGIERI, *Web 2.0. Il web tra legislazione e giurisprudenza*, Milano, Apogeo, 2008, e altro materiale dello stesso autore in unacademy.ning.com/video/diritto-e-nuove-tecnologie-7.

[33] La notizia è comparsa su sito della Rensselaer http://news.rpi.edu/update.do?artcenterkey=2410&setappvar=page%281%29 ed è poi rimbalzata in varie testate giornalistiche sparse nel mondo.

per la lettura delle *chat* testuali degli altri utenti e da rumori ad hoc che indichino l'avvicinarsi o l'allontanarsi di uno o più avatar dal proprio"[34].

Entrare in un metaverso è relativamente facile, più difficile è uscirne.

Non è un caso che l'avatar venga considerato "immortale". Informaticamente parlando la morte di un avatar equivale alla cancellazione del suo *account*. In SL l'opzione è prevista dalla LindenLab, ma per abbandonare il "gioco" occorre una comunicazione al gestore della piattaforma e il pagamento di una somma di denaro (vero) necessaria perché il proprio avatar cessi di esistere.

Nel sito di SecondLifeItalia[35] in proposito si legge: "A seguito della cancellazione del vostro *account basic* risulterà un pagamento pendente di circa 10USD. Questo pagamento è dovuto nel solo caso in cui si decidesse di riattivare il proprio *account*, diversamente non sarà necessario pagare alcunché a Linden Lab." In questo modo è assicurata la cancellazione del proprio *alter ego*, il nome e cognome e quindi, sostanzialmente, la propria identità virtuale. Ci si chiede che fine facciano tutti i dati e le informazioni che l'avatar ha rilasciato oppure ha raccolto durante la sua effimera esistenza. Si spera che vengano terminati insieme alla sua identità, ma non c'è una certezza su questo, in quanto incredibilmente sono pochi quei soggetti che decidono di abbandonare SL cancellando il proprio avatar e preferendo, piuttosto, abbandonarlo ad una triste sorte di dormiente (nell'ambiente l'inattività viene etichettata con il termine *away*)[36].

3. Le attività in *Second Life*

In un mondo virtuale l'individuo può decidere di riproporre gli stessi rapporti professionali o commerciali che ha nel mondo reale.

Per capire come si sviluppa l'aspetto economico nei mondi virtuali occorre conoscere il funzionamento di un metaverso. Prendiamo ad esempio il più conosciuto: *Second Life*.

[34] "Anche i non vedenti su *Second Life*", in http://punto-informatico.it/2071761/PI/Brevi/anche-non-vedenti-second-life.aspx.

[35] V. http://www.secondlifeitalia.com/wiki/Quanto_costa.

[36] Questa forma di "abbandono" a volte genera una sensazione di disagio, perché col tempo si tende ad instaurare con il proprio avatar un vero e proprio legame, a metà tra l'affettivo e lo strumentale. La nostra immagine in 3D a volte è percepita come un segno che ci identifica e contraddistingue e dunque si finisce con il considerarla come una parte di noi.

Per entrare in SL è necessario creare un proprio avatar con cui interagiranno tutti gli altri utenti, anch'essi sotto forma di avatar. Ogni avatar ha una serie di caratteristiche-base comuni e altre più sofisticate che variano a seconda degli accessori di cui il "titolare" intende dotarlo, con il passare del tempo oppure a seconda delle proprie esigenze. Tra le caratteristiche comuni c'è la possibilità di muoversi all'interno di SL volando da un'isola all'altra[37]; di interagire con i propri simili attraverso una *chat* (*virtual chat*) attraverso la quale dialogare[38].

Altra caratteristica comune a tutti gli avatar è la possibilità di fare acquisti pagando con il Linden$ che è la moneta "locale" (oppure con denaro vero direttamente dalla Linden Lab), questa moneta circola attraverso un sistema (informatico) di accreditamento da un *account* all'altro (in apparenza da un avatar-acquirente ad un avatar-cedente).

Solo se si è residente si possono effettuare acquisti e investimenti più consistenti, come ad esempio l'acquisto di un lotto di terreno virtuale. La residenza si ottiene depositando al momento della iscrizione a SL (*leggi* Linden Lab), una somma vera di denaro (in realtà sono piccole quantità corrispondenti a pochi dollari); se ciò non accade si è automaticamente considerati "cittadini di serie b" e in tal caso le uniche cose che si possono fare sono: giocare o effettuare piccoli acquisti, non si possono svolgere attività professionali né fare del *business*.

L'unico diritto unanimemente riconosciuto in SL è il diritto d'autore. L'avatar è un *software* e così anche i vestiti, le movenze, gli acquisti, la costruzione di oggetti e/o di case, le cessioni di beni … tutte queste cose sono prodotte da *software*. Una vera Bengodi per gli informatici e, forse, non è un caso che molti dei personaggi che si sono arricchiti in SL siano programmatori che hanno venduto gli *script* dei propri oggetti creati appositamente per essere utilizzati nel mondo virtuale.

[37] Il territorio in *Second Life* è strutturato su una serie infinita di isole. Gli avatar possono acquistarle ed edificare su di esse, oppure utilizzarle a proprio piacimento. Lo spostamento da un luogo all'altro, in genere, avviene con una sorta di teletrasporto (che ricorda molto l'ambiente di *star trek*) semplicemente digitando il nome della località di SL nella finestra *"edit-search"* del sito, oppure le coordinate del luogo dove si vuole essere trasportati.

[38] In questo modo il dialogo fra due o più personaggi avviene in chiaro, nel senso che tutti possono vedere (=sentire) ciò che viene detto, a meno che i due avatar dialoganti non decidano di parlare in privato attivando una opzione che nasconde il dialogo (c.d. modalità IM).

In questo contesto ogni utente ha il diritto d'autore sugli "oggetti" che crea cioè sul prodotto del proprio ingegno. Questi "prodotti" possono essere venduti o semplicemente scambiati tra gli avatar.

Sul diritto d'autore occorre precisare che in *Second Life* il concetto di proprietà rispecchia e subisce l'influenza del digitale. Non si acquista mai completamente un prodotto perché essendo in presenza di un *software* la cessione di un oggetto (da parte dell'autore) non avviene mai completamente, ma semmai si permette la creazione di una o più copie dell'originale. Si attua, cioè, una concessione del proprio diritto. Rifkin direbbe che i metaversi come SL rendono naturale ciò che nella *real life* sarebbe disastroso e cioè la consapevolezza che concetti come la proprietà, sono completamente superati a causa dello sviluppo di una società basata sempre più sulla fruizione di servizi piuttosto che sul concetto di un loro "possesso".

In SL gli oggetti circolano muniti di "permessi"[39] che pongono limitazioni al loro utilizzo. In questo modo l'autore etichetta il proprio prodotto "flaggandolo" e attribuendogli un livello di concessioni di copia corrispondente a quello che si vuole concedere e con cui si vuole che il proprio prodotto circoli *in-world*.

Il *business* in SL non riguarda solo questo aspetto che comunque resta il più eclatante. Molto del successo di questi metaversi dipende dal fatto che essi sostanzialmente rappresentano un formidabile strumento di comunicazione, aggregazione e scambio di idee. SL, ad esempio, è ormai comunemente utilizzato dagli utenti non più soltanto per scambiarsi file musicali e video, ma anche per svolgere convegni, lezioni, per fare informazione e per sondaggi o *exit poll* legati alla politica[40].

Commercio on line

Nei metaversi come SL è possibile svolgere attività di *e-commerce* passando dal tradizionale ambiente *web*, bidimensionale, in cui l'acquirente

[39] Ricordano i DRM Digital Rights Management.

[40] Nel 2007 fu fatto un esperimento, dalla segreteria del Partito Democratico, attraverso l'allestimento di seggi in SL per la scelta del proprio candidato. SLURL http://slurl.com/secondlife/Italianieuropei/50/146/24.

sceglie il prodotto ed effettua il pagamento, ad un ambiente più sofisticato, in 3D, dove l'acquirente entra fisicamente in uno spazio di contrattazione e acquista direttamente attraverso il proprio avatar. Tutto ciò grazie alla realizzazione di un contesto grafico amichevole di interazione tra *software* all'interno di un complesso sistema informatico.

In questo tipo di transazioni la contrattazione telematica può evolversi in forme contrattuali più complesse, cibernetiche, in cui l'intelligenza artificiale assume un ruolo principale sostituendosi (o nella migliore delle ipotesi integrando) alla volontà umana dei contraenti[41].

Nei metaversi i problemi legati alle transazioni virtuali sono di due tipi: l'aspetto tecnico della sicurezza offerta dalla piattaforma digitale utilizzata nei pagamenti e il controllo degli imprenditori e dei prestatori di servizi che operano nell'ambiente in 3D.

Nella vendita di beni o nella fruizione di servizi reali, l'acquisto avviene spesso rinviando all'ambiente *web* aziendale (e quindi utilizzando i classici sistemi di *e-commerce*), mentre l'accertamento dell'identità degli operatori commerciali appare complesso e aleatorio. Alcuni operatori del settore suggeriscono il ricorso a sistemi di controllo già presenti in altre piattaforme vagamente simili, come eBay, in cui la creazione di associazioni di cyberconsumatori (*Virtual World Business Bureau*) ha lo scopo di difendere gli utenti da possibili truffe. Alcuni metaversi prospettano soluzioni più tecniche, come in Entropia Universe dove la moneta interna (il PED[42] simile ai *lindendollar* di SL) è provvista di un proprio ID (= identificativo unico) che ne permette la mappatura durante la sua circolazione anche nell'eventualità del cambio con la moneta reale. La Lindenlab invece assicura che la propria piattaforma è in grado di monitorare tutte le trans-

[41] Sugli agenti *software* cfr. G. SARTOR, *Gli agenti software: nuovi soggetti del diritto*, in "Contratto e impresa", n. 2, 2002, pp. 465 e ss.; ID., *L'intenzionalità degli agenti software e la loro disciplina giuridica*, in "Rivista trimestrale di diritto e procedura civile", n. 1, 2003, pp. 23 e ss.

[42] Il PED (Project Entropia Dollar) è la valuta utilizzata all'interno di Entropia Universe. Corrisponde alla decima parte di un USD (United States Dollar), per cui: 10 PED equivalgono ad un dollaro statunitense. In Entropia esiste anche una PED-card che è una vera e propria carta di credito in-game. Viene fornita al giocatore all'atto della registrazione. Non può essere venduta, ceduta, smarrita oppure usata da altri giocatori; è utilizzata per acquistare oggetti nei negozi in-world oppure nelle aste o, ancora, per effettuare scambi diretti con altri giocatori.

azioni che avvengono in moneta locale, fino al punto di riconoscere e intercettare scambi "sospetti"[43].

Il lavoro

In SL alcune esperienze lavorative finiscono per diventare reali e possono rappresentare una fonte di reddito e di guadagno tutt'altro che virtuale[44]. L'offerta, in questi ambienti, non è poi molto diversa da quella del mondo reale e così, pur essendo sia il lavoro sia le figure professionali del tutto virtuali il compenso pattuito può essere in moneta reale e il corrispettivo può venire versato direttamente sul conto corrente dell'individuo "in carne e ossa"[45].

Le forme di lavoro puramente virtuale in un metaverso del tipo SL possono variare in riferimento al tipo di soggetto/avatar che ne fa richiesta.

I *newbie*[46], ad esempio, possono cercare di guadagnare nei *camping chairs*[47], nelle *dance pads*[48] (pedane circolari), oppure possono scegliere tra

[43] Cfr. *Second Life* Magazine in http://www.2litaliaworld.it/pdfrivista/2L_4.pdf.

[44] È il caso di Diana, doppiatrice nella vita reale che in Sl ha trovato un'altra occupazione diventando speaker e conduttrice di un telegiornale; oppure Vaniglia Oh, avatar di Arianna che ha lasciato il proprio impiego presso un portale *web* diffuso a livello nazionale per dedicarsi alla consulenza di comunicazione, marketing e didattica in *Second Life*, come riportato da A. BETTINI, *Vi presentiamo il nostro avatar. E il virtuale è più reale del previsto*, in "La Repubblica" del 10 agosto 2007, ww.repubblica.it/2007/04/sezioni/scienza_e_tecnologia/second-life-news/presentazione-avatar/presentazione-avatar.html.

[45] Nel 2007, la Randstad, multinazionale nel settore della ricerca delle risorse umane creò una propria filiale su *Second Life*, http://slulrl.com/secondlife/randstad/50/100/50. Erano tre le figure professionali richieste: un manager degli Avatar impegnati in uno studio legale olandese e due manager di hostess virtuali presso la sede virtuale di ABN AMRO. È possibile vedere il video promozionale su youtube http://www.youtube.com/watch?v=k5xF43POYv8 .

[46] È un novellino, ossia un nuovo utente, deriva dalla contrazione dei due termini *New* e *Beginner*.

[47] Letteralmente "sedie da campeggio". Sono sedie che vengono posizionate dagli *owner* della land nei pressi di negozi, piazzette e Casinò. Il lavoro dell'avatar consiste nello stare seduto su di esse per un certo periodo (indicato al di sopra della sedia). Alla fine del tempo previsto l'avatar riceve in cambio della sua "presenza" nella land un corrispettivo (più che un vero e proprio stipendio). Ovviamente queste *chairs* servono al gestore della land per incentivare il traffico di avatar nella propria isola. Per gli avatar è un gioco in cui si guadagnano linden ma per il titolare della terra è uno stratagemma per attirare "gente" che popoli il suo ambiente.

[48] Simili alle *chairs* hanno la forma di piattaforme. Salendoci sopra l'avatar incomincia a muoversi per le animazioni che vi sono contenute e che solitamente riproducono passi di

forme variegate e fantasiose di prestazioni, ad esempio: lavavetri o lavapavimenti, musicisti da strada, giardinieri, cubisti, abbracciatori (in questo caso, il guadagno consisterebbe nell'offrirsi di abbracciare, dietro compenso, chi ne faccia richiesta. L'avatar esibisce un cartello con scritto "offresi abbraccio", chi vuole essere abbracciato paga un compenso); un altro sistema per guadagnare qualche linden sta nel proporsi come cadavere (letteralmente: *head shot* ossia "fare il cadavere". In questo caso il "lavoro" consisterebbe nello stare immobili, sdraiati, come morti e circondati da una sagoma di gesso) oppure, più semplicemente, come pensatore[49].

In questi casi ovviamente la paga è bassissima: un massimo di 3 linden per circa 10 minuti di posizione. Pur sempre un guadagno se si considera che si viene ricompensati per "non fare nulla".

Si possono ottenere anche lavori più specializzati che non richiedono una approfondita conoscenza di SL, come il commesso/a, il ballerino/a professionista, il modello/a, il buttafuori, la guardia e l'escort!

I lavori che richiedono una certa professionalità, oltre che una padronanza dell'ambiente digitale, sono preceduti da un colloquio e successiva "assunzione" da parte del "datore di lavoro"[50], rientrano in questa categoria le figure del programmatore, dello stilista, dell'architetto, del dj o dell'organizzatore di eventi.

Infine, la libera professione in SL può comprende sia i professionisti sia gli imprenditori, presenti con le proprie agenzie immobiliari, attività di compravendita di terreni, *broker*, ecc.

Le regole d'uso della *land* nella quale si intende lavorare rappresentano una sorta di "legge-quadro" che i privati debbono rispettare nello svolgimento della loro attività relazionale con gli altri abitanti della stessa isola, spesso variano da *land* a *land* ma hanno, a loro volta, come riferimento le regole di uso della Linden Lab.

ballo. È un'attività che può essere fatto da chiunque, e per questa non è richiesta alcun tipo di colloquio di lavoro.

[49] Le modalità di ingaggio consistono semplicemente nel cliccare con il tasto destro del mouse rispettivamente: Sit-here - clean - scrub - Dance - Guitar - Garden – Meditation. Tutte indicazioni che ora si trovano anche in italiano sulla piattaforma in lingua italiana. Per saperne di più cfr. http://www.secondlifeitalia.com/wiki/Lavoro.

[50] Per trovarle occorre cercarle nella sezione *Classifieds del Search*.

Nel 2007, da una inchiesta di *Business Week*[51], rivista settimanale di economia, emerse che coloro che avevano scelto di abbandonare il proprio lavoro nella vita reale, spostando la propria attività esclusivamente in quello virtuale[52] erano riusciti a guadagnare anche il triplo in più.

In realtà, una simile possibilità è abbastanza remota, ma per la Linden Labs rappresenta comunque un'ottima forma di pubblicità.

In effetti, i personaggi che si sono arricchiti in SL non sono molti:

- Ailin Graef è una di questi nuovi Paperon de' Paperoni del metaverso, una donna il cui avatar è conosciuto come Anshe Chung. La sua fortuna ha avuto origine da una straordinaria lungimiranza nell'investire 10 miseri dollari per acquistare 400 lotti di terra virtuale rivendendoli poi a 1.200/1.600 dollari (reali) l'uno[53];

- Rueben Steiger, nome dell'avatar Reuben Millionsofus, ha guadagnato ingenti somme di denaro (vero) diventando consulente di marketing per grossi clienti, il suo lavoro consiste nell'aiutare (a pagamento) aziende o privati (per lo più politici che intendono farsi pubblicità in *Second Life*) ad interfacciarsi con questo mondo virtuale. Tra i suoi clienti la Microsoft, la Toyota, la Coca-Cola, la Warner Bros;

- Sibley Verbeck (in SL Sibley Hartor) che ha fondato la Electric Sheep Company con 55 dipendenti, offre consulenza e disegna palazzi e avatar per grandi società (Cbs, Sony, e altre);

- Alyssa LaRoche (Aimee *Web*er) ha iniziato disegnando vestiti e, organizzando feste, poi ha fondato una vera e propria azienda, la Aimee *Web*er Studio; ha creato una marca di abbigliamento, la Preen, e ora si fa pagare per aiutare le aziende (reali) che vogliono aprire un loro spazio su *Second Life*;

- Kevin Alderman (avatar Stroker Serpentine) grazie al porno è diventato uno dei più ricchi imprenditori di CyberSex dopo aver venduto su eBay il quartiere (virtuale) a luci rosse di Amsterdam (da lui stesso ricreato in SL) per 50.000 dollari (veri).

[51] Cfr. http://images.businessweek.com/ss/07/04/0416_richlist/index_01.htm?chan=technology_special+report+—+virtual+life_virtual+life.

[52] Cfr. *Second Life*: *c'è chi ha lasciato il lavoro reale per dedicarsi solo a quello virtuale*, in "Digitallex.com", http://www.digitallex.com/index.php?option=com_content&task.

[53] V. il sito http://www.anshechung.com/.

Tutto ciò porta a formulare un ardito latinismo: "*Ubi moneta ibi ius*" e a dedurre, come conseguenza logica, la necessità di un diritto in *Second Life*. In proposito Peter Ludlow[54], professore di Filosofia e Linguistica all'Università del Michigan, si è espresso negativamente affermando che una simile cosa "Non funzionerebbe mai". Anche lui frequentatore di *Second Life* e con un proprio avatar (Urizenus Sklar), ad una specifica domanda, durante un'intervista, sulla possibilità di un sistema legale virtuale in grado di regolamentare comportamenti e transazioni in SL, ha risposto che è molto più facile "che si crei un sistema per dirimere le dispute basato sulle leggi del clan e delle tribù".

Probabilmente non è un caso che gli unici professionisti assenti (o quasi) da SL sono proprio gli operatori del diritto. Tuttavia è difficile credere che, a lungo andare, un sistema come SL possa fare a meno di un apparato di norme giuridiche e di fonti legislative vere, in grado di creare e assicurare regole valide a tutela degli avatar residenti che in realtà sono degli investitori economici in carne e ossa. Fino ad ora le uniche regole sono quelle imposte dal sistema e dal regolamento contrattuale della Linden lab[55] che gestisce l'intera piattaforma informatica. In questo schema "tribale" molto semplice ma che in realtà trova la sua fonte in un vero e proprio contratto, in cui si confrontano una parte forte (la Lindel lab) e una parte patologicamente più debole (i singoli utenti), ad ogni avatar viene riconosciuto un unico forte diritto: il diritto di proprietà sui propri prodotti e, come corollario, il diritto connesso di commercializzarlo direttamente.

A lungo andare sarà la stessa esigenza di mercato (ossia il bisogno di sicurezza nelle transazioni e negli scambi) a spingere metaversi simili a *Second Life* verso forme di tutela meno aleatorie e più giuridiche. Sarà lo stesso imprenditore che investe in questi ambienti digitali a chiedere di vedere tutelato il proprio investimento, affinchè sia massimizzato, attraverso l'imposizione di regole "non solo economiche, del mondo che va creando". Non dimentichiamo, infatti, che molti dei metaversi digitali (che non si limitano ad essere semplici giochi di

[54] Riferito da M. GEROSA, *Second Life,* Melteni, 2007, pp. 93 e ss.

[55] Cfr. http://secondlife.com/corporate/tos.php.

ruolo) sono l'espressione speculare della vita reale e proprio per questo sarà naturalmente presente in essi la tipica conflittualità interpersonale degli esseri umani. In SL, ad esempio, le proteste da parte di alcuni avatar per l'acquisto di oggetti poi rivelatisi difettosi, con richiesta di restituzione del prezzo, sono previste attraverso lo strumento di "denuncia di abusi", appositamente predisposto dalla Linden Lab. Ma spesso questa pratica si è rivelata inutile.

In una notizia un pò datata[56] alcuni esperti dell'ICANN in occasione dell' *Influence Forum* del 2007[57] hanno evidenziato come giochi del tipo *The Sims Online* possono diventare interfacce destinate ad essere strumenti "di riferimento per ogni tipo di impresa", perdendo la loro iniziale funzione meramente ludica in quanto "Servizi, B2B, pubblicità e altri settori si affideranno sempre di più a soluzioni giocose"[58].

Sempre più spesso si pensa di proporre all'utente che decide di svolgere i suoi acquisti in rete, un ambiente virtuale semplice nell'utilizzo, immediato nei rapporti intersoggettivi grazie alla presenza di avatar, insomma un ambiente che riproduca la vita reale il più fedelmente possibile. Un luogo che vada oltre l'automatico *point and click* del *web* o il freddo contatto per e-mail e che rassicuri, anche psicologicamente, l'utente riproponendo un ambiente familiare popolato da soggetti con cui interagire in modalità sincrona come accadrebbe in real life.

4. I METAVERSI E IL DIRITTO. AMBITI E SETTORI GIURIDICI COINVOLTI

Gli ambiti e i "settori" giuridici che risentono dell'impatto tecnologico del digitale sono diversi. Da un punto di vista penale è possibile che vengano commessi reati in un metaverso. Questi reati possono essere ordinari, ma commessi attraverso lo strumento tecnologico, oppure "virtuali".

Rientrano nella prima ipotesi le previsioni del furto, in cui gli avatar vengono derubati del proprio credito; oppure l'ipotesi di diffusione di

[56] "L'e-commerce passa per SIMS e *Second Life*.", News di Dario D'Elia martedì 11 settembre 2007 in http://punto-informatico.it/2061703/PI/News/e-commerce-passa-sims-second-life.aspx.

[57] Cfr. http://www.influenceforum.com/.

[58] Cfr. http://www.techcrunch.com/2007/09/08/virtual-worlds-are-the-future-of-global-commerce-icann-ceo.

virus volto a danneggiare un *software* o un sistema informatico come nei casi, molto comuni in SL, della perdita di controllo del proprio avatar a causa dell'utilizzo di un programma malevolo fornito da malintenzionati sotto forma di regalo. L'ingiuria e la diffamazione in *Second Life* si concretizzano come le altre ipotesi più note in rete, sia attraverso l'uso della *chat* locale utilizzata dagli avatar per parlare tra di loro sia, in casi più sofisticati, viva voce, qualora si usufruisca di apposito programma. Sono possibili, inoltre sia la violazione di domicilio informatico sia l'appropriazione di credenziali di autenticazione di un altro avatar.

Lo scambio tra avatar di materiale pedopornografico, nei metaversi simili a SL, si concretizza nel caricamento, *download*, e circolazione di immagini oscene o comunque a contenuto sessuale.

Cambia lo scenario, dunque, ma il contenuto resta identico a quello del mondo reale[59].

Anche lo sfruttamento della prostituzione può essere presente in SL. Una sentenza della Cassazione del 2006[60] ha delineato nuovi scenari in materia di prostituzione virtuale riconoscendo il reato di sfruttamento della prostituzione anche in assenza di contatto fisico. Secondo la Cassazione infatti: "L'atto di prostituzione non implica di necessità la congiunzione carnale, comunque realizzata, o anche il solo contatto fisico tra i soggetti del rapporto, dovendosi invece far coincidere la relativa nozione con quella, assai più ampia, di prestazione sessuale a pagamento, qualificabile come tale ogni qual volta essa consista in comportamenti oggettivamente idonei a stimolare l'istinto sessuale del fruitore" con la ulteriore precisazione che "qualsiasi prestazione sessuale effettuata dietro corrispettivo, senza che la prestazione sessuale debba necessariamente consistere nella "congiunzione carnale": infatti, qualsiasi attività diretta a eccitare e soddisfare la libidine sessuale del destinatario si configura come 'prestazione sessuale' e integra prostituzione se è appositamente retribuita dal destinatario della medesima".

Dai reati veri e propri si giunge ad ipotesi più blande, come ad esempio il semplice *griefing*, ossia un'attività svolta da un soggetto (giocatore) che

[59] Per altre informazioni cfr. E. BERLINGIERI, *op. cit.*

[60] Cass. Pen., 21 marzo 2006, n. 346 con note di C.A. ZAINA in http://www.altalex.com/index.php?idnot=34117 e di S. MARANI, in http://www.altalex.com/index.php?idnot=34993.pdf.

tende ad irritare e molestare gli altri giocatori, piuttosto che a perseguire gli obiettivi di gioco[61]. Rientrano in questa ipotesi: la violenza sessuale nei confronti di un avatar oppure l'avataricidio, termine di indubbio effetto ma privo di fondamento giuridico. La sostanziale differenza tra il mondo reale e quello virtuale, basata sull'assenza della fisicità, rende, infatti, impossibile riconoscere una simile forma di violenza. L'unica ipotesi, in questo caso e in casi simili, resta il riconoscimento di una semplice forma di disagio, sconcertante e fastidiosa ma non paragonabile ad un reato.

Tra i "crimini virtuali" c'è il *racket* virtuale.

Circola la voce, in SL, del ragazzo che dopo un promettente inizio di attività di tatuaggi, in seguito a minacce e richieste di pizzo ha dovuto abbandonare la professione[62]. Gli strumenti realizzati dai cybermafiosi per intimorire i clienti erano *software* in grado di scaraventare gli avatar lontano dalla bottega del giovane imprenditore. Anche qui il caso, se vero, non può essere equiparato ad un crimine ma piuttosto ad uno scherzo fastidioso, un *griefing* appunto, basato sull'utilizzo dannoso di *script* o di veri e propri *software*.

L'unica forma di tutela è il ricorso alla c.d. *netiquette*, composta da standard predefiniti di comportamento che sono presenti un pò in tutti i metaversi, SL inclusa.

In quasi tutti i metamondi la tutela e la vigilanza sono autogestiti dagli stessi residenti, una sorta di "fai da te" che spesso si concretizza nel ricorso a *software* in grado di controllare l'accesso e bloccarlo agli indesiderati. Un pò come viene fatto dai moderatori nelle *chat*.

Ben diverso è il discorso sulla sicurezza nazionale e sul terrorismo. Qui non c'è *griefing* che tenga e non è passata inosservata la preoccupante notizia apparsa un paio di anni fa sulla comparsa di movimenti jihaddisti in SL, "Secondo i timori di polizie e servizi segreti di diversi paesi, le organizzazioni del terrorismo islamico potrebbero usare il sempre più frequentato mondo virtuale di Internet per reclutare adepti e compiere attentati virtuali a scopo propagandistico"[63]. È proprio il caso di dire che qui il "gioco" si fa duro.

[61] Da Wikipedia - en.wikipedia.org/wiki/Griefer.

[62] M. Bono, *Dalla pedofilia al "pizzo"*, in milano.repubblica.it/dettaglio/second-life-il-paradiso-perduto/1304905, sezione Tecnologia & Scienza, 10 maggio 2007.

[63] La notizia è datata 2007, "Virtual jihad hits *Second Life web*site" di Chris Gourlay and Abul Taher riportata in www.timesonline.co.uk/tol/news/world/middle_east/article2199193.ece.

In ambito civilistico le problematiche più eclatanti sono essenzialmente di due tipi: quelle legate alla tutela della persona e quelle collegate a forme di responsabilità (civile) per eventuali danni e relativa imputabilità.

Nell'ipotesi di tutela della persona si può spaziare fra ambiti ormai più che noti e già regolamentati come ad esempio la *privacy* e i diversi diritti della personalità quali: il diritto alla propria identità, il diritto alla identificabilità, il diritto all'anonimato, il diritto ad agire e vivere in sicurezza e ad esprimere la propria personalità senza limiti od ostacoli in qualsiasi comunità si decida di operare (reale o virtuale che sia).

Un discorso a parte merita il diritto di proprietà che, in *Second Life* può riguardare il rapporto con il proprio avatar o con i prodotti creati *in-world*. L'argomento investe, inevitabilmente, anche gli aspetti inerenti al diritto d'autore (sia morale sia patrimoniale) e quello ancora più specifico di tutela del marchio (laddove vi siano pericoli di violazioni e abusi, o forme di concorrenza sleale) sfociando, così, nello specifico ambito del diritto industriale.

5. Il diritto e le tutele

Si può tentare di semplificare il rapporto tra diritto e mondo virtuale riconducendolo a due aspetti: a) il verificarsi di ipotesi in cui, pur operando in ambiente digitale, si viola la legge del mondo reale; b) l'ipotesi in cui si opera in un mondo virtuale infrangendo regole virtuali o comunque di semplice *netiquette*.

Nel primo caso è possibile, forse con qualche difficoltà interpretativa, ricondurre le situazioni prospettate al diritto positivo.

Nel secondo caso l'ostacolo è rappresentato dal fatto che nei metaversi del tipo SL non ci sono istituzioni né regole abbastanza forti da diventare *super partes* e rappresentare, quindi, uno strumento adeguato di tutela per dirimere controversie tra avatar. In SL, ad esempio, esistono standard di comportamento che si rifanno alla *netiquette* e quindi agli usi consolidati tra utenti, oppure è possibile ricorrere a forme contrattuali di *agreement* predisposte unilateralmente dalla Linden lab. Non si è mai ritenuto opportuno adottare una "costituzione" o un codice *ad hoc* oppure organizzare strutture che potrebbero essere definite "paragiuridiche" e cioè simili a tribunali a cui ricorrere in caso di bisogno da parte dei titolari degli avatar.

Da ricordare, tuttavia, che forme di autoregolamentazione in caso di controversie sono ormai giuridicamente riconosciute sia attraverso strumenti di prevenzione, come i codici di condotta, sia con la previsione di sistemi di risoluzione delle controversie *on line* (ODR), entrambi applicabili anche in ambienti virtuali come SL.

La responsabilità in Second Life

In una società dell'informazione è prevista una responsabilità da parte del c.d. fornitore di servizi.

La normativa di riferimento a livello nazionale è il d.lgs. n. 70 del 2003 che recepisce le indicazioni europee emanate con la Direttiva 2000/31/CE (sul commercio elettronico). Il d.lgs. 70/2003 negli artt. 14 (Responsabilità nell'attività di semplice trasporto - *Mere conduit*), 15 (Responsabilità nell'attività di memorizzazione temporanea - *Caching*), 16 (Responsabilità nell'attività di memorizzazione di informazioni - *Hosting*) e 17 (Assenza dell'obbligo generale di sorveglianza) specificamente prevede sia le varie tipologie di *provider* sia le relative forme di responsabilità. In realtà il legislatore ha operato attraverso un meccanismo che potremmo definire "al negativo", trattando i casi di "non responsabilità" e facendo costantemente riferimento a tutte quelle ipotesi in cui certamente il *provider* non debba considerarsi responsabile, mentre tace (per una effettiva difficoltà di determinazione) sulla identificazione di forme di responsabilità. Pertanto l'interprete può procedere solo comparando se le ipotesi che gli vengono sottoposte siano ricomprese tra le forme di non responsabilità, e solo in caso negativo ritenere il *provider* imputabile dei danni cagionati. Sostanzialmente il *provider* non ha obblighi di controllo su quello che gli utenti fanno all'interno del proprio *server* in quanto è effettivamente difficile, se non impossibile, riuscire a monitorare l'enorme flusso dei dati.

Il legislatore europeo ha avuto l'accortezza di suddividere le varie ipotesi evidenziando il caso in cui il *provider* sia comunque coinvolto nei contenuti e nella gestione dei dati; unico caso, questo, in cui dovrà essere chiamato a risponderne (art. 16 d.lgs. 2003).

La Direttiva europea, prima, e il d.lgs. italiano di recepimento, poi, hanno tentato di dare una risposta corretta ai tentativi che all'epoca furono fatti, di trovare a tutti i costi un responsabile, punendo l'unico soggetto che era effettivamente identificabile in rete e cioè il *provider*.

Nel caso specifico di SL la Linden lab, paragonabile alla figura del *provider*, tende a risolvere eventuali conflitti attraverso meccanismi di autoregolamentazione, come, ad esempio, la segnalazione degli abusi attraverso la sezione di "*Abuse Report*" (segnalatore gli abusi). Questa opzione è, tuttavia, riservata ai soli residenti e ad essa può seguire l'applicazione, all'avatar segnalato, di una sanzione meramente virtuale che consiste nel bannare l'utente fastidioso dal sistema[64].

Nelle regole d'uso (termini di contratto), dette anche ToS[65], della Linden, al punto 12, dedicato alle ipotesi di risoluzione delle controversie, si legge che è nell'intento della stessa società di dirimere rapidamente le eventuali controversie, in base sia al meccanismo ADR, se l'importo non supera i 10.000 dollari, sia ricorrendo alla legge della California, (…) o alla Convenzione delle Nazioni Unite sulla vendita internazionale di merci.

La privacy

Conservare la propria *privacy* in un ambiente altamente tecnologico è una pia illusione. Le ipotesi di violazione o di attentato alla propria sfera privata sono infinite e variegate e spesso è lo stesso utente che le permette perché di fatto ignora gli strumenti tecnologici utilizzati.

In SL, ad esempio, è una prassi comune offrire e accettare proposte di amicizia fra avatar, attività che viene denominata *friendship*. Ma non sempre si ha consapevolezza che accettando l'amicizia di un avatar di fatto si permette a questo di conoscere ogni nostro movimento *on line*. Così come avviene in altri ambienti digitali, come ad esempio nei sistemi di messaggistica istantanea. L'opzione di "rintracciabilità" è spuntata di *default*, solo chi ha un pò più di dimestichezza (o presta semplicemente maggiore attenzione) può impedire che ciò accada, togliendo il *default*. Ci sono, poi, altri strumenti più sofisticati che permettono di monitorare la nostra presenza *on line* nonostante qualsiasi precauzione.

A coloro che obiettano che *privacy* e libertà devono convivere si fa presente che senza un diritto forte in grado di tutelare sia l'una sia l'altra, la

[64] Ma nulla vieta a costui di rientrarvi con altra identità.

[65] Cfr. la versione Terms of Service aggiornata al 2010, http://secondlife.com/corporate/tos.php.

convivenza diventa difficile se non impossibile. Lo stesso Garante della *privacy* si è espresso più volte in merito, emanando raccomandazioni in parallelo con gli interventi delle Autorità di garanzia europee. Tra queste si citano il Memorandum di Roma[66] del 2008 e la Risoluzione sulla tutela della *privacy* nei servizi di *social network*[67], anch'essa del 2008; entrambi documenti che pur trattando di *social network* possono considerarsi come riferimenti validi da applicare ad altri tipi di ambienti digitali.

In SL la *privacy* è regolamentata nei paragrafi 9 e 14 del ToS, rispettivamente: "Privacy and Your Personal Information" e "Additional Terms and Policies", quest'ultimo articolato in ulteriori sottosezioni, tra le quali si nota un "Additional Terms and Policies" che sviluppa in modo più analitico quanto enunciato nella precedente versione dei termini d'uso. Sostanzialmente viene ribadito che la Linden Lab raccoglie e utilizza i dati personali al fine di migliorare il servizio offerto e che si impegna a proteggere la *privacy* dei propri utenti e ad utilizzare i loro dati personali come descritto nella Privacy Policy. Questo rinvio conduce il (certosino) lettore alla relativa sezione "Privacy Policy" che è, a sua volta, piuttosto dettagliata (consta di sette "capitoli"[68]), nella quale viene ribadito che la Linden Lab si impegna a proteggere la *privacy* dei propri utenti al fine di mantenere con loro un forte legame di fiducia. Sempre nell'ambito di questa specie di introduzione della sezione sulla *privacy*, la società precisa che la raccolta e la conservazione dei dati ha come fine quello di fornire i servizi e predisporre e mantenere una piattaforma sicura e protetta. Nella sezione che tratta delle modalità di raccolta e di trattamento dei dati, viene spiegato che queste vengono effettuate in due modalità: la prima, diretta-

[66] Nel sito del Garante della *privacy* http://www.garanteprivacy.it/garante/doc.jsp?ID=1567124, Rapporto e Linee-Guida in materia di *privacy* nei servizi di social network, "Memorandum di Roma", Adottato in occasione del 43mo incontro, 3-4 marzo 2008, Roma, dal Gruppo di lavoro di Berlino che si occupa della protezione dei dati nel settore delle telecomunicazioni.

[67] Nel sito del Garante della *privacy* http://www.garanteprivacy.it/garante/doc.jsp?ID=1560428 e adottata il 17 ottobre 2008 a Strasburgo dai 78 Paesi partecipanti alla 30ma Conferenza internazionale sulla protezione dei dati.

[68] Intitolati: The Information We Collect and How We Collect It; Linden Lab's Protection and Disclosure of Your Information; Information Displayed to or Collected By Other Users; Linden Lab's Use of Cookies; Third Party Advertisements; Disclosing Personal Information in Profiles, Forums or within *Second Life*; Amendment of This Policy.

mente, attraverso una richiesta all'utente, nella fase della registrazione, l'altra per "deduzione" (c.d. raccolta indiretta), effettuata attraverso le attività svolte nella piattaforma da parte dell'utente. È, questa, la tipologia più interessante, perché permette di raccogliere e conservare tutti i dati relativi all'*account*, ai *log* di *chat* o IM, all'indirizzo IP e *file* di *log*, ai luoghi visitati in *Second Life*, e ai dati che riguardano le "transazioni" svolte in piattaforma. Il tutto appare effettuato con una estrema disinvoltura.

La proprietà

Come già accennato, la proprietà nei metaversi non solo è riconosciuta, ma anche fortemente tutelata.

Ultimamente, tuttavia, contravvenendo a tutte le precedenti posizioni assunte dalla Linden lab in merito alla proprietà intellettuale sembra che i nuovi termini di uso riformulati nell'aprile del 2010 non riconoscano un pieno diritto sulle proprietà acquistate o create nel gioco dagli utenti.

La proprietà intellettuale sui propri prodotti è regolamentata al paragrafo 7 Termini di Uso (ToS), rubricato *Content Licenses and Intellectual Property Rights*. In questa sezione viene riconosciuto agli utenti del servizio da parte della Linden lab un diritto esclusivo sui prodotti che creano all'interno di *Second Life*, ossia qualsiasi diritto d'autore e di altri diritti di proprietà intellettuale nei confronti di qualsiasi contenuto creato utilizzando il servizio, purché, sostanzialmente, possano essere forniti alcuni diritti di licenza alla Linden Lab e *royalties* alla società che gestisce il sistema.

La formazione e l'apprendimento

È bene ricordare come, oltre all'aspetto meramente ludico, la didattica e l'insegnamento siano le principali vocazioni di *Second Life*.

Soprattutto nei Paesi di origine anglosassone SL viene considerata una piattaforma digitale dove impiantare campus oppure sperimentare nuove forme di didattica e di ricerca.

In effetti, le Università possono sfruttare le potenzialità dei metaversi come *Second Life* oltre che per l'apprendimento, anche per informare e comunicare o per creare comunità più o meno complesse che fungano da strumento aggregante tra studenti e/o docenti, dando vita ad una forma di *social learning*. In Italia sono ancora poche le Università[69] che credono e soprattutto investono nei metaversi. Il primo ateneo italiano ad essere presente in SL è stato quel-

lo di Torino che ha creato una propria *land* (Unito), mentre sono molti gli esperimenti extra-universitari che riguardano, comunque, la formazione o la ricerca[70]. Nel maggio del 2009 si è celebrato un evento particolarmente atteso nell'ambiente dei metamondi, la prima laurea ottenuta frequentando un corso svolto interamente in ambiente virtuale. La laurea è stata assegnata a Julia Shannan e ciò che ha piacevolmente sorpreso è stato il fatto che la prima laurea reale ottenuta in modo virtuale è stata conseguita da una donna[71].

6. I CASI GIURISPRUDENZIALI

La giurisprudenza, soprattutto quella statunitense, si sta interessando solo negli ultimi anni del fenomeno dei mondi virtuali. Di seguito si riportano alcuni tra i casi più curiosi.

Primo caso di studio. Utente di Second Life *contro la* Linden lab[72]

La causa è del 4 ottobre 2006 ed è stata intentata da Marc Bragg contro la Linden Lab davanti ad una Corte della Pennsylvania. Qualcuno ha considerato il caso come l'espressione della ennesima follia degli avvocati americani, in considerazione del fatto che Marc Bragg è un avvocato della Pennsylvania con la passione dei MMORPG.

I fatti sono questi: la Linden lab ha sospeso l'*account* di Bragg e ne ha confiscato i terreni (virtuali) in seguito al sospetto di guadagni (una com-

[69] Alcune di queste: l'Università degli Studi di Torino, (Unito 128,108,24), l'Università degli Studi di Cagliari (Unica 55,111,4010), il Laboratorio di Simulimpresa (Perting SRL) della Facoltà di Economia di Forlì dell'Università di Bologna (Kouhoun 223,250,53), il Dipartimento Ingegneria Elettrica e dell'Informazione della Facoltà di Lettere e Filosofia dell'Università degli Studi dell'Aquila (Adrift 140,21,47), l'Università di Catania, Osservatorio per la comunicazione e interazione in SL, in collaborazione con Nuova Sicilia (272,204,43).

[70] Tra i tanti v. unAcademy in http://unacademy.ning.com/video/didattica-in-sl-parte-12.

[71] Nel Texas State Technical College's virtual college (vTSTC), la notizia in www.pr*web*.com/releases/TSTC/virtual_education/pr*web*2419874.htm. È possibile vedere il video su youtube al seguente indirizzo: www.youtube.com/watch?v=AUi-_C7N_5g&eurl=http%3A%2F%2Fwww%2Eavatarexperience%2Eeu%2Findex%2Ephp%3Foption%3Dcom%5Fcontent%26view%3Darticle%26id%3D268%253Aprima%2Dlaurea%2Dvirtuale%26catid%3D55%253Amondi%2Dvirtual&feature=player_embedded.

[72] Cfr. www.chescolawyers.com/; *Il terreno virtuale finisce in tribunale*, in "Punto informatico", 2006 (punto-informatico.it/1816609/PI/News/terreno-virtuale-finisce-tribunale.aspx).

pravendita) illeciti. L'avvocato ha ritenuto esistessero i presupposti per adire l'autorità ordinaria citando la Linden Lab per la restituzione dei beni confiscati, la riassegnazione del proprio *account*, e cioè la reintegra del proprio avatar, all'interno di SL e un risarcimento danni di ottomila dollari per la confisca di "beni" che nella vita reale si attestano sul valore di diecimila dollari (veri).

L'aspetto più interessante non è rappresentato (come è stato gridato dai giornali) dall'eventuale riconoscimento di un diritto di proprietà su di un bene virtuale[73], ma piuttosto dal fatto che viene violata la proprietà intellettuale che l'utente-autore ha sulle proprie creazioni circolanti nel metaverso. Diritto peraltro riconosciuto dalla stessa Linden lab. La violazione consisterebbe nell'incauto atteggiamento "punitivo" (congelamento *account* e confisca dei beni) della Società che gestisce la piattaforma digitale.

Altro spunto di riflessione deriva dal fatto che per la prima volta viene richiesto l'intervento di un tribunale "vero" il quale, peraltro, ha ritenuto particolarmente grave l'illecito prospettato evidenziando come la causa sia degna di rispetto e respingendo, dunque, la richiesta della Lindenlab di dirimere la controversia attraverso lo strumento arbitrale. L'ipotesi infatti configurerebbe una palese violazione della tutela del consumatore[74] attuando di fatto uno squilibrio contrattuale alla base del rapporto tra società Linden e consumatore. Le stesse condizioni di utilizzo del servizio offerto dalla società che gestisce il metaverso riconoscerebbero una posizione dominante di quest'ultima nei confronti dell'utente.

Secondo caso di studio. Tu mi lasci e io ti uccido[75]

Il caso si è verificato in Giappone. Anche qui lo scenario è solo in apparenza virtuale. Il metaverso che fa da sfondo alla storia questa volta non è SL ma Maple Story che, come SL, permette ai propri utenti di sposarsi virtualmente.

[73] Che non ha corrispondenza nel mondo reale e che perciò non esiste.

[74] Con riferimento alle condizioni generali di contratto e alle clausole vessatorie e abusive.

[75] V. GENTILE, *Uccide un avatar. Arrestata*, in "Punto informatico", 2008 in http://punto-informatico.it/2452340/PI/News/uccide-un-avatar-arrestata.aspx.

In seguito ad un divorzio altrettanto virtuale, uno dei due cyber-coniugi decide di vendicarsi del torto subito rubando l'*account* del suo *ex* e cancellando dal MMPORG il suo avatar inducendolo a fare *harakiri*. Nell'ipotesi, ovviamente, ciò che ha interessato il giurista non è stato il "suicidio" virtuale, quanto il verificarsi dell'accesso e la sostanziale manipolazione di dati da parte di un utente non autorizzato. Il gesto ha avuto come logica conseguenza una condanna. Vera.

Terzo caso di studio. Come è facile copiare in Second Life[76]

L'oggetto del contendere è, in questo caso, la violazione del *copyright*. Viene scoperto, in SL, un "applicativo 'clonatore' di oggetti che, infiltrandosi nelle comunicazioni *client-server*, è in grado di intercettare i dati e replicare qualsiasi oggetto del metamondo". Questo applicativo è conosciuto con il nome di CopyBot. Il tool, predisposto dalla stessa Lindenlab (con la collaborazione di una società *open source*, la Libsecondlife), aveva come fine quello di identificare i bug nel sistema di sicurezza del metamondo, ma ha finito con l'essere modificato come sistema utile a clonare. Gli utenti hanno così dovuto munirsi di un *software* anti-CopyBot, lamentando, inoltre, nei confronti della Linden lab poca attenzione alla tutela della proprietà privata dei propri utenti.

A sua volta, la Lindenlab ha dichiarato che non è possibile ritenere responsabili dei danni provocati dal CopyBot gli sviluppatori bensì coloro che in malafede lo utilizzano per scopi illeciti (nel caso specifico per effettuare copie non autorizzate di oggetti creati da altre persone).

La società, inoltre, molto diplomaticamente, si è dichiarata disponibile ad affiancarsi a coloro che si ritengono danneggiati qualora intendano effettuare azioni legali alla luce di quanto disposto dal DMCA (Digital Millennium Copyright Act).

La Lindenlab si è fatta, in questo specifico caso, promotrice di una interessante proposta che trova il suo fondamento nella filosofia *open source*. In riferimento ai principî *open source*, infatti, anche la copia e la manipolazione di un *software* o di altro prodotto, quando viene effettuata per ampliarne le

[76] G. BOTTÀ, *Second Life travolto dai pirati?*, in "Punto informatico", 17 novembre 2006, in http://punto-informatico.it/1764602/PI/News/second-life-travolto-dai-pirati.aspx.

potenzialità, diventa essa stessa espressione di creatività. Pertanto, se l'attività di copia e manipolazione di un *software* (o altro prodotto) è svolta per migliorarne le caratteristiche potrebbe perdere la caratteristica di "illiceità" e diventare a sua volta oggetto di tutela.

La società ha auspicato, in questo caso l'applicazione di forme di licenze *copyleft*, come le Creative Commons, in grado di prevedere il riconoscimento all'autore sul prodotto originario e al contempo permettere a terzi di migliorarne le potenzialità, riconoscendo in capo ad essi la paternità delle modifiche innovative apportate ma anche le relative responsabilità.

7. La morte dei metaversi

I metaversi come *Second Life*, in questi ultimi tempi, sembrano in crisi. Ci si chiede se valga veramente la pena avere una seconda vita, un secondo lavoro o una seconda attività aziendale in un metaverso.

I numeri dei c.dd. residenti (gli avatar attivi) dal 2007 (periodo di massimo splendore) ad oggi sembrano essersi ridotti notevolmente[77]. Da sondaggi effettuati emerge che le *land* di grandi marchi come Best Buy, Sun Microsystems, Dell, Coca Cola, Nike, Ibm, Microsoft, Nissan, Sony sono pressochè deserte. Appare sempre più chiaro che il vero motivo per cui molte aziende decidono di entrare e investire in un mondo virtuale come *Second Life* non è l'effettivo riscontro economico quanto la necessità di non trovarsi escluse da nessuna forma di *business*.

Eppure, nonostante tutto, i rapporti tra SL e RL continuano. Nel metaverso italiano nascono le riproduzioni speculari in 3D di città come Mantova, la prima città italiana a comparire in SL seguita da Torino (con la realizzazione di Italia Vera). Artisti di ogni tipo utilizzano sempre più spesso SL per ambientarvi le loro *performance* come è accaduto a Irene Grandi e Paola e Chiara. In SL vengono riprodotti siti di interesse storico o artistico come la Basilica Palladiana, di Palazzo Barbaran Da Porto e della Villa Cordellina della provincia di Vicenza che ha realizzato nel 2008 un progetto denominato "Park Palladio"[78] presentato al Parlamento Europeo e inaugurato con la benedizione virtuale dell'avatar del Vescovo

[77] J. D'Alessandro, *Tanta pubblicità, pochi abitanti quel bluff chiamato SL*, in "La Repubblica", 13 agosto 2007.

di Vicenza Cesare Nosiglia alla presenza degli avatar del Presidente della Provincia di Vicenza Attilio Schneck e dell'Assessore all'Innovazione, Politiche Giovanili , Servizi Legali, Sistemi informatici, Organizzazione Logistica, Sportelli decentrati Andrea Pellizzari. In Park Palladio sono inoltre presenti 7 sportelli virtuali, nei quali vengono ricevuti i visitatori dal personale dei rispettivi enti negli orari indicati nelle targhe. Un progetto all'avanguardia che, nell'ambito degli interventi previsti dal piano di *e-government*, prevede l'erogazione di servizi al cittadino (in via sperimentale il rilascio dei tesserini per la raccolta dei funghi e le autorizzazioni per le licenze di pesca).

Anche i nostri politici utilizzano sempre più spesso *Second Life* come ulteriore canale di comunicazione politica. Il primo ad aprire una conferenza politica e a comprare un terreno è stato Antonio Di Pietro (2007).

Tra le Regioni italiane la prima a sbarcare in SL è stata la Toscana.

La prima isola italiana della IBM è stata aperta nel 2007.

Nel 2007 in occasione di un congresso medico fu trasmessa in SL la prima operazione chirurgica di ernia inguinale[79], mentre dal 21 ottobre 2008 al 7 gennaio 2009 al Museo di Storia Naturale di Firenze si è svolta all'interno di *Second Life* la mostra Rinascimento virtuale.

In SL nascono anche testate editoriali, tra queste la rivista italiana 2L Italia[80], fondata da Alessandro Rossini, rilevata e pubblicata nel 2007 da Maggioli Editore che possiede anche FreeLife Magazine, sempre dedicata a *Second Life* ma in lingua inglese.

8. Conclusioni

Dall'analisi effettuata emerge una attenta riflessione sul rapporto tra persona e regole giuridiche e sull'ancor più profondo concetto di "centralità dell'uomo".

Come ogni innovazione tecnologica anche i metaversi (e nel nostro caso *Second Life*) vedono schierarsi, a favore oppure contro, la comunità

[78] Le coordinate in SL sono: Park palladio 136, 121, 24. La notizia è ripresa da http://www.provincia.vicenza.it/notizie/salastampa.php/8674.

[79] V. http://punto-informatico.it/2075796/PI/News/ernia-inguinale-second-life.aspx.

[80] Nel sito all'indirizzo http://www.2litaliaworld.it/ è riportato l'avviso che "è attualmente in manutenzione".

scientifica, ma al di là di ogni valutazione positiva o negativa che si intende fare è innegabile che l'utilizzo di queste piattaforme tridimensionali ha una enorme importanza dal punto di vista culturale.

Grazie ad esse è possibile per chiunque, qualsiasi abilità abbia l'individuo, muoversi e partecipare ad innumerevoli eventi sociali: visitare musei e gallerie d'arte, assistere a presentazioni di libri, ascoltare concerti, frequentare lezioni e seminari a distanza, offrire la propria professionalità, i propri servizi o prodotti e scaricare o acquistare libri da librerie virtuali senza spostarsi da casa.

La rete aperta: riflessioni sui valori e le regole dell'innovazione 2.0

GUIDO DI DONATO*

SOMMARIO: *1. Società in rete e tecnologia dell'informazione – 2. Paraordinamentalità delle reti virtuali e processi di comunicazione aperta – 3. Innovazione 2.0 e nuova economia dell'informazione – 4. Innovazione infrastrutturale fra regolamentazione e mercato – 5. Internet e cyberdemocrazia – 6. Innovazione collaborativa ed organizzazioni eterarchiche*

1. SOCIETÀ IN RETE E TECNOLOGIA DELL'INFORMAZIONE

Ha scritto il sociologo Anthony Giddens: "andare incontro ad una fase di postmodernità significa allontanare la traiettoria dello sviluppo sociale dalle istituzioni della modernità e puntare verso un nuovo e diverso tipo di ordine sociale[...] Il postmodernismo, ammesso che esista in forma cogente, può esprimere la consapevolezza di tale transizione ma non dimostra che essa esiste"[1]. In termini analoghi, il postmoderno ha designato senza gradualismo un percorso di sviluppo tecnologico e scientifico, con ricadute immediate sulla vita quotidiana e sulla politica. Così, nel trascorrere degli anni, la radicalizzazione della modernità è diventata la conseguenza più evidente di un processo di evoluzione sociale scandito dalle tecnologie dell'informazione e dalla rivoluzione digitale.

Con una discontinuità che ha segnato indelebilmente il dinamismo dell'attuale panorama economico e culturale è mutato il nesso di immedesimazione tecnologia-società. Si è fatto più stringente e ineludibile, fino a trasformarsi in un'equazione ove non è più possibile rappresentare la società senza i suoi strumenti tecnologici[2]. La loro naturale dislocazione è ormai collocata nell'inedito meta-racconto di una nuova era[3], fra que-

* L'Autore è docente di "Regolazione delle reti, privacy e tutela dell'opera multimediale" presso la Facoltà di Scienze della comunicazione dell'Università degli Studi "La Sapienza" di Roma ed è responsabile della Funzione Sicurezza Territoriale - Area Centro della Telecom Italia Spa.

[1] A. GIDDENS, *Le conseguenze della modernità*, Bologna, Il Mulino, 1994, pp. 52-59.

[2] W.F BIJKER, T.P HUGHES, T. PINCH (eds.), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, Cambridge, MIT Press, 1987, pp. 113-133.

[3] J.F. LYOTARD, *La condizione postmoderna*, Milano, Feltrinelli, 1981. Secondo l'Autore, il progetto della modernità, di conferire un senso unitario e globale alla realtà, individuandone

stioni aperte e potenti forme di "intelligenza collettiva e connettiva"[4], che riguardano non più soltanto la pratica comunicativa o l'artefatto tecnologico, ma investono direttamente i processi di "modellamento sociale"[5].

Le tecnologie informatiche concretizzano mutamenti che toccano l'antropologia stessa delle persone (viste appunto come *networked persons*)[6], in un contesto che attiva e disattiva in modo selettivo gli individui, le comunità e persino le nazioni, a seconda della rilevanza loro attri-

i fondamenti e facendo leva su una scienza unitaria, si è costruito sull'asse di tre grandi metaracconti: illuminismo, idealismo, marxismo. Così P. GIORDANETTI, *Lyotard e l'entusiasmo storico politico,* in http://itinera.unimi.it/mat/saggi/html.

[4] L'originale confronto filosofico riguarda le posizioni critiche espresse da P. LEVY e D. DE KERCHOVE nell'intervista *Due Filosofi a confronto. Intelligenza collettiva e intelligenza connettiva: alcune riflessioni*, in http://www.mediamente.rai.it/home/bibliote/Intervis/d/dekerc05.htm. Si veda in tal senso anche P. LEVY, *Cyberdemocrazia. Saggio di Filosofia Politica*, a cura di G. Bianco, Milano, Mimesis, 2008, p. 183; P. LEVY, *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, Milano, Feltrinelli, 1996. In particolare secondo Levy: "l'intelligenza collettiva è data dalla memoria collettiva, da un immaginario collettivo. Siamo quel che siamo grazie all'esistenza delle istituzioni, delle tecniche, dei linguaggi, dei sistemi di simboli, dei mezzi di comunicazione. La nostra intelligenza individuale è totalmente infiltrata dall'intelligenza collettiva; non saremmo intelligenti se non usassimo il linguaggio, se non fossimo stati allevati in una certa cultura". L'opinione di De Kerchove è invece riportata nel seguente passaggio**:** "un artista australiano, Ross Harly, mi disse che io non esprimevo l'idea di un'intelligenza collettiva, perché facevo riferimento, nelle mie riflessioni, ad un sistema di connessione aperta. Non si trattava di riferirsi ad un contenitore chiuso, ma ad una connessione da persona a persona all'interno di una rete molto specifica. Questa connessione con la sua specificità che non sta nel contenitore collettivo di un sapere, di una conoscenza, di uno scambio, mi suggerì di chiamarla "connettiva". Questo concetto è formidabile per capire i processi che la tecnologia digitale ha apportato, e mi ha permesso di scoprire l'intelligenza, o, meglio, l'inconscio connettivo ricco di possibilità. Continuo a prendere ispirazione dal lavoro di Levy e cerco di coinvolgerlo alla pratica diretta tramite l'intelligenza connettiva. Una vecchia battuta di Molière in "Les femmes savantes" recita in questo modo: "Un gentiluomo è qualcuno che sa tutto senza avere imparato niente". Penso che con Internet, con il Web e con l'accesso che abbiamo a questa intelligenza collettiva, a questa base cognitiva, siamo tutti dei gentiluomini. Possiamo avere accesso a tutto senza avere imparato mai niente. Ciò è divertente, fa parte del piacere di appartenere della nostra epoca, di essere legati a questa formidabile memoria collettiva". In tal senso anche D. DE KERCHOVE, A. CURSI (a cura di), *Dopo la democrazia? Il potere e la sfera pubblica nell'epoca delle reti,* Milano, Apogeo, 2006*;* D. DE KERCHOVE, V. SUSCA*, Transpolitica nuovi rapporti di potere e di sapere*, Milano, Apogeo, 2008.

[5] F. PASQUALI, B. SCIFO (a cura di), *Consumare la rete, la fruizione di internet e la navigazione del web*, Milano, V&P, 2004, pp. 27 e ss.

[6] S. RODOTÀ, *La vita e le regole*, Milano, Feltrinelli, 2009, pp. 89 e ss.

buita nel raggiungere gli obiettivi prioritari, elaborati nelle reti di comunicazione elettronica[7].

La questione è aperta e si sposta pertanto anche sui confini contigui e sui terreni più ripidi della possibilità morale di riprogrammare il concetto stesso di empatia umana[8]; di rimodulare uno stato di coscienza, che per millenni si è esercitato entro cerchie troppo ristrette (dalla famiglia alla comunità agricola, fino allo Stato-nazione) ed isolate dalle dimensioni globali delle attuali *community* interconnesse e planetarie.

In questo processo cognitivo, la rete diventa un nuovo luogo dell'essere, con un *ethos* dell'interattività in grado di produrre condivisione, cooperazione, confronto e critica serrata nelle attività più diverse; dalla scienza alla produzione industriale, fino alla coscienza sociale. Uno spazio sconfinato in cui sta diventando possibile ripensare la natura stessa dell'uomo e ricostruire la civiltà di un mondo frammentato, bisognoso di radicali ristrutturazioni e di nuove forme di organizzazione personale e sociale.

La riconciliazione delle logiche opposizionali esistenti tra l'io e la rete, tra il mondo reale e quello virtuale, tra la comunicazione computer mediata e la tutela giuridica dell'identità e della socialità tangibile[9], nonché di taluni diritti fondamentali di libertà, rappresentano pertanto il punto di partenza di questa personale pratica di ricerca. Per converso, lo snodo centrale in cui essa si colloca, riguarda lo studio delle piattaforme Internet, come spazio di innovazione economica, tecnologica e anche giuridica.

L'ampio e roboante dibattito scientifico, avviato da tempo su queste tematiche, è stato troppo spesso dominato da una visione lineare dello sviluppo della tecnologia e da un'ingiustificabile e fuorviante scissione, tra teorizzazioni sui progressi tecnologici, da un lato, e società dall'altro. Il collegamento esistente fra i due elementi è invece strettissimo, e solo focalizzando l'attenzione sullo studio dei nuovi attori sociali (*users*) e dei nuovi contenuti della rete, (*networking* multidirezionali costruiti da milioni di mittenti/destinatari di messaggi), ci si pone nella condizione di rico-

[7] M. CASTELLS, *La nascita della società in rete*, Milano, Egea, 2008, p. 3.

[8] La teoria esposta è contenuta nell'ultimo saggio di J. RIFKIN, *La civiltà dell'empatia*, Milano, Mondadori, 2010.

[9] Ampio panorama del tema in R. MESSINETTI, *Identità e comunicazione. Profili di diritto civile*, Torino, Giappichelli, 2007.

struire correttamente il rapporto di interazione esistente fra tecnologia dell'informazione e società.

La traiettoria tecnologica rappresenta, infatti, una variabile decisiva del percorso evolutivo di una società che attraverso lo Stato – pur non determinando la tecnologia – diviene comunque in grado di accelerarne lo sviluppo. Un futuro che si costruisce con processi di modernizzazione ed interventi di *public policy* per la realizzazione di infrastrutture abilitanti (la larga banda e più in generale le reti infrastrutturali) e piattaforme tecnologiche (Internet), in grado di assicurare rapidi e radicali cambiamenti economici. Allo sviluppo del libero mercato sarebbe così sufficiente affiancare un sapere tecnico analogo a quello che le scienze applicano ai fenomeni naturali[10].

Non è facile, tuttavia, stimare empiricamente l'impatto delle *Information Comunication Technologies* (ICTs) sulla crescita economica di un sistema paese. Il metodo, in estrema sintesi, prende in considerazione le tecnologie abilitanti (classificate come *General Purpose Technologies* o GPTs)[11] con maggior impatto sull'evoluzione di un sistema economico e con ricadute anche indirette in tutti i settori della società che le utilizzano[12]. L'indice di sviluppo di tali tecnologie (reti infrastrutturali e piattaforme) diventa quindi il principale indicatore per gli studi econometrici che analizzano l'impatto delle ICTs sulla produttività e su altre variabili, come la crescita dei livelli occupazionali, dei salari ed infine dello stesso PIL, soprattutto nella prospettiva dei paesi in via di sviluppo[13].

[10] Così J. HABERMAS, *Tecnica e scienza come ideologia*, in "Teoria e prassi nella società tecnologica", Bari, Laterza, 1978, IV edizione, dove l'Autore ha esaminato, in particolare, i diversi aspetti del collegamento esistente tra il sapere tecnico scientifico ed il mondo vitale nelle società a "capitalismo maturo".

[11] Sono considerate come storiche GPTs: l'elettricità, la macchina a vapore, il motore a scoppio, le ferrovie, ecc.

[12] Con specifico riferimento all'impatto della banda larga sulle variabili indicate si vedano: R.W. CRANDALL, W. LEHR; R. LITAN, *The Effects of Broadband Deployment on Output and Employment: A Cross Sectional Analysis of US Data*, in "Issues in Economic Policy, The brooking Institution", 6, pp. 2-35; P. KOUTROUMPIS, *The Economic Impact of Broadband on Growth. A Simultaneous Approach,* London, Mimeo, Imperial College, 2008; C.Z.W. QIANG, C.M. ROSSOTTO*, Economic Impacts of Broadband*, Washington DC, World Bank, 2009.

[13] Sul tema si veda l'ampia trattazione di R.G. LIPSEY, C. BECKAR, K. CARLAW, *The Consequences of Changes in GPT's*, in Helpman E. (ed.), "General Purpose Technologies and

In questa catena aperta si colloca, infine, un ultimo anello: la valutazione della storia sociale dell'Information Communication Technology, come mezzo attraverso cui ridisegnare Internet, anche come categoria descrittiva e strumento di analisi antropologico culturale[14]. Ciò soprattutto, nello studio dei cd processi di *domestication*, che nella sociologia dei media misurano la diffusione della tecnologia nelle unità domestiche e spiegano come si realizza l'incorporazione (o addomesticamento) delle ICTs nella vita quotidiana dell'uomo comune[15].

2. Paraordinamentalità delle reti virtuali e processi di comunicazione aperta

In un inedito e articolato scenario, la spinta dell'innovazione digitale sta effettivamente ridefinendo, non solo le dimensioni spazio-temporali della società e dell'economia (declinate ormai in termini di *cybertime* e *cyberspace*)[16], ma anche quelle del diritto. I problemi giuridici legati ai vari sistemi di *con-*

economics Growth", Cambridge, MIT Press 1998; nonché L. Pupillo, *Impatto della banda larga sulla crescita economica: evidenze della letteratura*, Telecom Italia - Columbia University, in "L'industria", XXX, n. 4, ottobre-dicembre 2009, pp. 710 e ss.

[14] Come osserva, infatti, C.T. Altan in *Soggetto, simbolo, valore*, Milano, Feltrinelli, 1990, pp. 46-47: "il tema più congeniale allo spirito dell'indagine antropologico culturale (…) sembra essere dato dalla speciale attenzione posta sullo studio dei fenomeni di costume, del sapere collettivo, delle credenze e dei valori e più in generale della mentalità condivisa dai membri, individui e gruppi, di una moderna società complessa, in rapporto ai problemi che la caratterizzano [...] Accade infatti spesso, per la ben nota vischiosità delle forme della cultura, che le fratture più gravi di conseguenze si stabiliscano fra la cultura tradizionale di un popolo e le nuove esigenze di gestione di un sistema economico sociale, fattosi ormai complesso nei modi che si sono descritti".

[15] R. Silverstone, L. Haddon, *Design and Domestication of Information and Communication Technologies: Technical Change and Everyday Life*, in Mansell R., Silverstone R., "Communication by Design", Oxford, Oxford University Press, 2008, pp. 44-74.

[16] Il termine cyberspazio, neologismo degli anni ottanta, si riferisce alla cibernetica (corrente scientifica transdisciplinare degli anni quaranta e cinquanta che ha consacrato le nozioni di informazione e comunicazione nel mondo scientifico). Ora, in maniera significativa, la cibernetica designa la scienza del "potere e del controllo", detto in altro modo la scienza del governo. In greco la parola *kubernétès*, che rappresenta altresì la radice etimologica del termine cambiamento, sulla quale N. Wiener si è ispirato per costruire "cibernetica", significa pilota, guida, colui che tiene il timone. Come dire non c'è guida (governo) possibile in assenza di un circuito di comunicazione, di uno spazio di circolazione dell'informazione che è appunto

tent management, come Facebook, Youtube e Flickr, sono numerosi, spesso poco chiari ed in alcuni casi tendono a non essere correttamente interpretati. Sembra quasi che la struttura tecno-futurista dell'esistenza, vissuta fino a ieri al riparo delle leggi dell'uomo, rifiuti oggi l'intervento della regola, per autopromuoversi al cospetto di un diritto a cui sarebbe disposta, al massimo a chiedere rassicurazione piuttosto che regolamentazione[17].

Strumenti di comunicazione aperta come *blog*, *social network*, motori di ricerca e nuove metodologie di fruizione della rete, come il *Web 2.0*[18], chiamano invece il giurista al cospetto dell'attualità e di nuovi dati di realtà (sui quali l'ordinamento non ha ancora avuto il tempo di maturare diritti acquisiti ed elaborazioni giurisprudenziali strutturate), elaborati da una scienza e da una tecnologia che mutano sistematicamente le forme e la sostanza della regolazione giuridica[19].

Si innesca così il frequente confronto con problematiche che gli ordinamenti giuridici ritengono di poter "normare" ma dove, in realtà, l'irrompere improvviso del diritto paga lo scotto dell'impossibilità di adeguarsi alla velocità dell'evoluzione tecnologica.

La regola giuridica, in altri termini, sembra perdersi nelle dimensioni paraordinamentali del mondo digitale, mentre il quotidiano uso della rete – figlio della co-regolamentazione orizzontale, di una matrice di parteci-

il cyberspazio. Il governo di una società passa per questo *cyberspazio,* nel senso ampio del termine, cioè per l'universo del linguaggio umano, così come esso è strutturato da una certa ecologia della comunicazione del momento contingente. Il cyberspazio costituisce pertanto il nuovo "centro" dove si accumulano le informazioni – un centro insolito in quanto si trova ormai ovunque in rete (Così P. LEVY, *Cyberdemocrazia*, cit., pp. 32-77).

[17] Così F. VIOLA, *Dalla natura ai diritti. I luoghi dell'etica contemporanea*, Bari, Laterza, 1997.

[18] II termine Web 2.0 è utilizzato per indicare genericamente uno stato di evoluzione di Internet (e in particolare del World Wide Web), rispetto alla condizione precedente. Si tende ad indicare come Web 2.0 l'insieme di tutte quelle applicazioni on line che assicurano un elevato livello di interazione sito-utente/utente-utente (*blog*, *forum*, *chat*, sistemi quali Wikipedia, Youtube, Facebook, Myspace, Twitter, Gmail, Wordpress, Tripadvisor ecc.). La locuzione pone l'accento sulle differenze rispetto al cosiddetto Web 1.0, diffuso fino agli anni novanta, e composto prevalentemente da siti web statici, senza alcuna possibilità di interazione con l'utente, ad eccezione della navigazione tra le pagine, l'uso delle *e-mail* e l'uso dei motori di ricerca. (http://it.wikipedia.org/wiki/Web_2.0).

[19] E. BERLINGIERI, *Legge 2.0. Il web tra legislazione e giurisprudenza*, Milano, Apogeo, 2008, pp. 13 e ss.

pazione attiva dei consociati, nonché di soluzioni sostitutive più efficaci della lentezza dei procedimenti legislativi – disconosce la forza del vincolo giuridico, con cui il legislatore tenta di colmare l'orrore dei vuoti normativi lasciati dalle leggi della natura[20].

Lungo questa via, ci imbattiamo nel dilemma di una trama semplice, lineare, già vista e facilmente intuibile nel corso della sua storia, ove il tentativo di adeguare le leggi alle tecnologie informatiche, mostra con straordinaria evidenza tutti i suoi limiti. Nasce così un diritto debole, per il quale Internet, *new medium* per antonomasia, rappresenta un ideale di natura aliena da cui, come un *avatar* nell'ultimo capolavoro del regista James Cameron, non riesce a farsi accettare. Sembra quasi che l'area critica si sia improvvisamente allargata e la rete che nel film interconnetteva la vita della flora e la fauna con gli abitanti del pianeta Pandora, si sia trasformata nel mondo reale, nella rete delle reti che ormai connette miliardi di utenti, in un processo di partecipazione attiva e totalizzante[21]. Una rete che nella finzione cinematografica aveva al suo centro un enorme salice che rappresentava il baricentro dell'universo, allo stesso modo in cui i computer e le moderne piattaforme costituiscono oggi il nucleo contenutistico essenziale della società postmoderna. Eccoci allora alla fine, proiettati ad intravedere un diritto in cerca di riparo in altri luoghi della comunicazione sociale, come in quell'albero delle voci, vivo e pulsante, dove i poetici *Woodsprite*, creature semi fluttuanti come meduse danzanti, risanavano le ferite agli abitanti della foresta pluviale.

Non a caso, ad epilogo di questo suggestivo percorso, è possibile rinvenire il riconoscimento giuridico dell'ingresso della tecnologia informatica nella società, proprio in quelle norme che si sono occupate di tutelare la riservatezza dell'individuo ed il suo diritto alla *privacy*, in relazione al

[20] A. CATANIA, *Metamorfosi del diritto. Decisione e norma nell'età globale*, Bari, Laterza, 2008, p. 172.

[21] Per una visione della rete delle reti, vista come incubatore democratico e strumento di partecipazione attiva del cittadino alla vita sociale del paese, si veda: M. CASTELLS, *Galassia internet*, Milano, Egea, 2006; C. FORMENTI, *Incantati dalla rete, immagini utopie e conflitti nell'epoca di internet*, Milano, Raffaello Cortina, 2000; G. LIVRAGHI, *L'umanità dell'internet le vie della rete sono infinite. Come usare la rete per arricchire le proprie esperienze e relazioni personali*, Milano, Hops Libri, 2001; S. RODOTÀ, *Tecnopolitica*, Roma-Bari, Laterza, 1997; C. CROUCH, *Postdemocrazia*, Roma-Bari, Laterza, 2003.

trattamento informatizzato dei dati personali ed alla tutela della vita privata nel settore delle comunicazioni elettroniche[22].

In tale ultimo ambito si colloca, infatti, la recentissima sentenza con cui il Tribunale penale di Milano ha condannato tre dirigenti del colosso informatico Google, per non avere impedito la diffusione, attraverso la piattaforma di *filesharing* YouTube, di un video contenente atti di bullismo perpetrati in danno di un disabile.

Il reato contestato si innesta nel combinato disposto degli artt. 110, 167 comma 1 e 2 del d.lgs 196/2003 (Codice *Privacy*), perchè gli stessi in concorso tra loro ed al fine di trarne profitto per il tramite del servizio *Google video*, avrebbero trattato dati personali, in violazione degli artt. 23, 17 e 26 dello stesso decreto, con relativo nocumento per la persona interessata. In aggiunta, il provvedimento precisa che nel caso in esame non può trovare attuazione la disciplina relativa alle esimenti contenute negli artt. 16 e 17 del d.lgs 70/2003, in quanto nel suo ambito di applicazione (art. 1, co. 2) "non rientrano… le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali".

In sintesi Google Italy avrebbe violato la disciplina sulla *privacy* sia per non aver adempiuto all'obbligo di informare correttamente gli utenti, in merito agli obblighi imposti dalla legge ed ai conseguenti rischi in caso di inottemperanza degli stessi, sia per non aver cancellato immediatamente i dati e le comunicazioni correttamente segnalate come criminose.

Le motivazioni della sentenza, pubblicate nei giorni scorsi, precisano infatti che "NON costituisce condotta sufficiente ai fini che le legge

[22] Il tema del *data protection* era già presente in alcuni progetti di legge negli anni ottanta. Il primo di questi fu il cd Progetto Accame, presentato alla Camera il 21 aprile 1981 e rubricato "Norme per la salvaguardia del diritto al rispetto della vita privata nei confronti dei sistemi di trattamento ed elaborazione automatica dei dati e delle informazioni". L'ingresso della disciplina nel nostro ordinamento, risale invece alla l. 31 dicembre 1996 n. 675. Il nuovo Codice Privacy introdotto con il d.lgs. 196/2003, dedica particolare attenzione allo specifico tema negli artt. 34, 51, 123 e 132, recependo così i principi contenuti nelle direttive 2002/58/CE e 95/46/CE. Allo stesso modo anche il nuovo codice delle comunicazioni elettroniche introdotto con il d.lgs. 259/2003, assicura la garanzia dei diritti inderogabili di libertà delle persone nell'uso dei mezzi di comunicazione elettronica (art 3), ribadendo le garanzie costituzionali di libertà di comunicazione e segretezza delle comunicazioni (art 4). Sullo specifico argomento: P. PERRI, *Privacy, diritto e sicurezza informatica*, Milano, Giuffrè, 2007.

impone, 'nascondere' le informazioni sugli obblighi derivanti dal rispetto della legge sulla privacy all'interno di 'condizioni generali di servizio' il cui contenuto appare spesso incomprensibile, sia per il tenore delle stesse che per le modalità con le quali vengono sottoposte all'accettazione dell'utente" ed inoltre che "tale comportamento, improntato ad esigenze di minimalismo contrattuale e di scarsa volontà comunicativa, costituisce una specie di 'precostituzione di alibi' da parte del soggetto/web e non esclude, quindi, una valutazione negativa della condotta tenuta nei confronti degli utenti".

Una superfetazione ermeneutica ribadita anche nella parte conclusiva del provvedimento, ove si sottolinea più volte che la condanna dei dirigenti di Google non viene costruita sulla base di un obbligo preventivo di controllo sui dati immessi, ma in relazione a un'insufficiente (e colpevole) comunicazione degli obblighi di legge, riguardo l'informativa sulla *privacy*.

In altri termini si è ritenuto che la corretta informativa agli utenti (anche se nel caso di specie si trattava da un'adolescente dodicenne, condannata con separato giudizio) e di conseguenza l'astratta possibilità, assicurata a questi ultimi, di poter acquisire il consenso di tutti i soggetti interessati (eventualmente coinvolti in un video contenente dati personali e sensibili, prima che questo venga diffuso *on-line),* rappresentano condizioni necessarie e sufficienti a garantire, nell'ambito di un'attività svolta con finalità lucrativa, l'adempimento degli obblighi richiesti dal codice *privacy*, al fine di evitare forme di responsabilità penale conseguenti all'illecito trattamento di dati personale e sensibili.

Fin qui, le argomentazioni giuridiche potrebbero trovare anche un presupposto di fondatezza, rinvenibile nello strumentale regime di garanzia e nel peculiare livello di protezione, riservato al trattamento dei dati sensibili dagli artt. 23 e 26 del d.lgs. 196/2003. Tuttavia la ricostruzione effettuata non chiarisce affatto i profili riguardanti la possibile violazione dei citati artt. 17 e 26, mentre è contraddittoria per quanto riguarda l'articolo 23. Il provvedimento si concentra sulla presunta mancanza di chiarezza nell'informativa sulla *privacy* ai sensi dell'art. 13, senza considerare, tra l'altro, che tale violazione non prevede una sanzione penale *ex* art. 167, ma si inquadra nel nucleo normativo delle sanzioni amministrative, contenuto nell'art. 161.

L'itinerario ermeneutico seguito nei successivi passaggi – al fine di rigettare la tesi accusatoria che avrebbe voluto Google Italy responsabile

anche di concorso in diffamazione – si pone inoltre in aperto contrasto con il precedente percorso argomentativo in tema di informativa, laddove asserisce che "anche se l'informativa sulla privacy fosse stata data in modo chiaro e comprensibile all'utente, non può certamente escludersi che l'utente medesimo non avrebbe caricato il *file* video incriminato, commettendo il reato di diffamazione".

La mancanza di coerenza logica, evidenziata nelle contraddizioni ripercorse dai descritti approdi interpretativi, si ripropone altresì nell'orientamento espresso in materia di responsabilità del *content provider* e dell' *host provider*. Secondo le richiamate motivazioni, ambedue i soggetti sarebbero sottoposti agli stessi obblighi ed alle stesse responsabilità, e ciò a prescindere da qualsivoglia ragionamento giuridico ma unicamente in quanto "Non esiste la sconfinata prateria di Internet dove tutto è permesso e niente può essere vietato, pena la scomunica mondiale del popolo del *web*. Esistono invece leggi che codificano comportamenti che creano degli obblighi che ove non rispettati conducono al riconoscimento di una penale responsabilità".

Applicato in quest'ottica, il rilevante precedente potrebbe addirittura configurare, a carico del fornitore di servizi di *hosting* (attività di memorizzazione di informazioni), anche un ulteriore onere rispetto a quelli già previsti dagli artt. 16 e 17 del d.lgs. 70/2003; ovvero quello di richiedere preventivamente, ai soggetti presenti in un qualsiasi video – direttamente o per il tramite dell'utente principale – il consenso alla pubblicazione delle loro immagini. Di contro, in caso di impossibilità di poterlo ottenere, o più semplicemente in mancanza di consenso, non dovrebbe invece essere consentita la diffusione di dati personali tramite *upload*.

L'eventuale violazione dei principî enunciati integrerebbe così una particolare forma di responsabilità del fornitore, derivante dal trattamento illecito dei dati personali (non solo sensibili) generati e diffusi dagli utenti.

Riscontrata l'esistenza di un nocumento all'identità personale ed alla *privacy* dell'individuo – richiesta quale condizione obiettiva di punibilità c.d. *intrinseca* – ed esclusa la configurabilità del caso di specie in termini di semplice violazione formale, ovvero di irregolarità procedimentale[23], la

[23] Cass., sez. III pen., sent. 28/05-9/07 2004, n. 1134.

decisione potrebbe dirsi altresì ispirata al principio costituzionale di prevalenza della tutela dei diritti inviolabili della persona (sicurezza, libertà e dignità umana) rispetto alla libertà di iniziativa economica, secondo lo schema tipico conformato dall'art. 41 della Costituzione.

L'area di operatività della fattispecie penale tuttavia, anche in questa ipotesi, subirebbe una dilatazione talmente estesa da trasformarsi in concreto in un "limite implicito" (in quanto non nominati nell'enunciato linguistico dell'art. 21 Cost.) alla libertà di manifestazione del pensiero. Tali particolari limiti, come noto, devono in ogni caso essere ricavati dall'interpretazione di altre disposizioni di rango costituzionale, in un giudizio di bilanciamento che, in ipotesi di contrasto fra attività individuali costituzionalmente rilevanti, stabilisca le condizioni di prevalenza e di compressione applicabili alla fattispecie concreta[24]. In aggiunta, il fatto stesso che la parte conclusiva del provvedimento auspichi l'approvazione di una "buona legge" che limiti la "libertà assoluta" della rete, evidenzia come il giudice non abbia tenuto conto nella propria decisione del principio generale del *notice and takedown* (ossia dell'obbligo di rimozione del contenuto illecito dopo un'appropriata segnalazione), perno fondante dell'intera normativa comunitaria sul commercio elettronico che trova altresì riscontro nella disciplina del diritto d'autore ed in particolare nel *Digital Millenium Copyright Act*.

La puntuale definizione dei confini operativi della disciplina e la richiesta di un giudizio di bilanciamento, in un ambito normativo di tale rilevanza, diventano pertanto esigenze prioritarie che inducono ad auspicare un intervento del Garante Privacy sullo specifico tema, anche per assicurare un orientamento interpretativo espresso *ratione materiae*, nelle more dei successivi ed eventuali gradi di giudizio.

Il tema della condivisione *on-line* di taluni aspetti della vita privata, resi pubblici attraverso *blog* e *social network,* apre così un nuovo spazio di riflessione giuridica, derivante dalla necessità di riconsiderare la portata degli strumenti di tutela della riservatezza della persona e del diritto all'autodeterminazione informativa[25], collocati in un più generale ambito di coesistenza tra tecnologia dell'informazione e diritto.

[24] R. MESSINETTI, *op. cit.*, pp. 38 e ss.

[25] Per il significato di questa espressione si veda S. RODOTÀ, *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in "Politica del diritto", 1991, pp. 101 e ss.

Da questo punto di vista, se è vero che la fenomenologia della comunicazione ha istituito un contesto di per sé rilevante per l'organizzazione attuale della società, ben si comprende come i livelli di senso descritti, nei quali si esprime la portata complessiva del fenomeno rete, abbiano condizionato anche l'evoluzione e gli usi sociali del diritto. Dobbiamo, dunque, fare i conti con una progressiva metamorfosi o degiuridificazione delle più tradizionali categorie dogmatiche, intessuta da profonde trasformazioni delle dimensioni quotidiane, oggetto dell'attenzione più intensa del giurista.

Il sasso è stato gettato ed affonda lentamente, proprio in quell'inedita complessità che rende manifeste vecchie aporie del diritto e altre ne fa esplodere[26]. È allora vero che l'era digitale sta trasformando le funzioni del diritto? E ancora, in futuro, potrà davvero la regola giuridica invadere l'universo virtuale e racchiudere Internet nelle *maglie d'acciaio* di un perimetro normativo? Oppure sarà la complessità dell'esistenza digitale a rivelare progressivamente le asimmetrie e gli scompensi di un diritto invadente in troppi settori e ciò nonostante assente là dove, in taluni casi, se ne avvertirebbe il bisogno[27]?

L'alternativa vive, in tutta la sua drammaticità, nei momenti di delegittimazione che colpiscono il legislatore quando il frutto del suo operato non si identifica con un sottostante orientamento sociale e lo svuotamento della capacità dello strumento giuridico evidenzia l'impossibilità, per quello stesso legislatore, di tener testa all'innovazione tecnologica.

L'assioma della crisi ordinamentale e della conseguente neutralizzazione giuridica inizia così a mostrarsi, in tutta la sua evidenza, soprattutto nella contrapposizione aperta che in tutto il mondo sta caratterizzando l'evoluzione della disciplina del diritto d'autore.

Come è noto, in Italia la materia è regolata dalla l. 22 aprile1941, n. 633, recante "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio". Si tratta di un testo risalente e frequentemente novellato, per rispondere alle esigenze prospettate dall'innovazione tecnologica, il cui impianto normativo è stato definitivamente incrinato dai potenti fendenti del mezzo digitale. Infatti, a fronte dell'inasprimento delle sanzioni

[26] A. CATANIA, *op. cit.*, pp. 5 e ss.

[27] S. RODOTÀ, *La vita e le regole*, cit., pp. 9 e ss.

previste dal legislatore, in caso di violazione del diritto d'autore ed in relazione ai tentativi di costruire una cornice criminale per le abitudini informatiche degli utenti, si sono andate progressivamente affinando nuove tecniche di fruizione e riproduzione (le c.d. nuove utilizzazioni o utilizzazioni successive) di beni digitali, attraverso l'affermazione di diffuse consuetudini *contra legem*.

In parallelo, per reagire ai vincoli della disciplina della protezione del diritto d'autore ed ai connessi divieti di condivisione di contenuti in rete, si sono costruite forme alternative di gestione dei diritti esclusivi, come le licenze *Creative Commons*, che assicurando la possibilità di utilizzare in modo libero e lecito opere protette o parti di esse, hanno segnato il passaggio epocale dalla rigidità formale dei mezzi di tutela del *copyright*, alla flessibilità delle concessioni in *copyleft*[28].

Nella stessa ottica, si inquadra la coeva affermazione dei paradigmi delle culture orizzontali (dette anche *Read & Write Web*[29]), teorizzate per sostenere la diffusione dei più recenti modelli di conoscenza convergente[30] e di fruizione di contenuti digitali aperti (c.d. Pubblicazioni ad acces-

[28] Permesso d'autore*,* termine introdotto dalle licenze *Creative Commons*. Queste licenze non sono altro che una forma contrattuale atipica di cessione di alcuni diritti di utilizzazione dell'opera che permettono alla generalità degli utenti determinati usi previsti dall'autore. In questo modo i diritti sono ceduti in via non esclusiva, non sono limitati ad un determinato ambito territoriale e favoriscono la circolazione in Internet di qualsiasi contenuto venga rilasciato con licenza di questo tipo. L'autore può decidere a quali condizioni tale circolazione può avvenire e tutti i diritti non compresi nella licenza rimangono soggetti all'autorizzazione dell'autore o dei suoi aventi causa. Le licenze Creative Commons, arrivate attualmente alla versione 3.0, sono caratterizzate da 4 attributi che combinati tra loro stabiliscono quali diritti d'autore rilasciare al pubblico. I 4 attributi sono: Attribuzione (*attribution*), Non Opere Derivate (*no derivatives*), Non Commerciale (*non commercial*), Condividi allo stesso modo *(share alike*). Da questi 4 attributi si ottengono 16 combinazioni, di cui solo 11 sono licenze valide. Di queste 11 solo 6 sono effettivamente utilizzate, poiché prevedono l'*attribution,* cioè il diritto morale alla paternità dell'opera che, come noto, non può essere eliminato. Così E. BERLINGIERI, *op. cit.*, pp. 120-127.

[29] Nel gergo attuale dei *geek* (appassionati di Internet) il termine Cultura RW, utilizza l'acronimo per indicare l'analogia con i livelli di autorizzazione attribuiti all'utente di un file digitale, ove il tipo RW (Read and Write/leggi e scrivi) indica la possibilità di modificare il file originario mentre il tipo RO (*Read Only*) consente esclusivamente la lettura del file.

[30] Per un'approfondita disamina del tema H. JENKINS, *Convergence Culture: Where Old and New Media Collide*, New York, NY University Press, 2006.

so aperto o più semplicemente Open Access[31]). In tale schema si ritrovano i milioni di utenti che ogni giorno rielaborano e scaricano dal *web* musica, testi, video e fotografie, trasformando la rete in uno straordinario spazio collaborativo ove si concretizza la possibilità di mettere a fattor comune nuovi contenuti, nati all'interno ed all'esterno dei suoi confini. Le opere dell'ingegno che ivi si riproducono, attraverso gli strumenti messi a disposizione dalla tecnologia e dai motori di ricerca – come avviene ad esempio in Google – aggiungono significato ai precedenti contenuti e generano innovazione culturale diffusa[32].

Ma, quasi paradossalmente, proprio nell'affermazione di queste nuove pratiche di interazione sociale, si cristallizza una controversia culturale senza precedenti, che vede ormai schierati, da un lato, i numerosi centri di interesse impegnati nell'affannosa ricerca di forme sempre più stringenti

[31] Il termine *Open Access*, nasce nel contesto internazionale della ricerca e in particolare della comunicazione scientifica. Si sta sviluppando in Europa da alcuni anni e recentemente è ormai giunto anche in Italia. È un movimento internazionale che incoraggia scienziati, ricercatori e studiosi a disseminare i propri lavori di ricerca rendendoli liberamente accessibili secondo due modalità:

- depositando il proprio lavoro o ricerca scientifica in un archivio aperto attraverso un processo noto come *self-archiving* o auto-archiviazione;

- pubblicando il proprio lavoro o ricerca scientifica su periodici ad accesso aperto, ossia quei periodici che offrono gratuitamente e senza restrizioni l'accesso agli articoli, a seguito di regolare processo di validazione (*referee*) in termini di qualità.

Con Accesso aperto alla letteratura scientifica si intende l'accesso libero via Internet alle produzioni intellettuali dei ricercatori e degli studiosi di tutto il mondo. Esiste anche una definizione ufficiale di Pubblicazione ad Accesso Aperto, nota come *Bethesda Statement on Open Access Publishing,* abbracciata e condivisa anche dalla *Public Library of Science*, da vari atenei e istituzioni britanniche e statunitensi, dallo *statement* del Wellcome Trust in supporto all' *open access publishing* e anche dall'IFLA, la Federazione Internazionale delle associazioni bibliotecarie (Così A. DE ROBBIO, *Open Access un movimento al centro di nuovi scenari di e governance*).

[32] Di parere contrario è la filosofa francese B. Cassin, secondo cui l'ideologia di Google può essere sintetizzata in un doppio motto: organizzare tutta l'informazione del mondo – operazione che Google spacciava come spuria di interessi e che andava curiosamente al passo con l'organizzazione e l'ordinamento geo-politico promosso dall'amministrazione Bush – e non essere cattivi, – imperativo che univa un *maximum* d'astrazione ad un *maximum* di pathos moralista, proprio come nella retorica neo-con dell'asse del bene. Così il caso Google – esempio paradigmatico della direzione verso la quale sta andando il cybermondo – diventerebbe un campione di democrazia culturale, ma senza cultura né democrazia. (B. CASSIN, *Google-moi. La deuxieme mission de l'Amerique*, Paris, Alben-Michel, 2007).

di tutela del diritto d'autore e dell'altro, la moltitudine di internauti, spesso impropriamente etichettati come "pirati", che intendono solo condividere liberamente il frutto delle relazioni sociali e dei loro *mash up* creativi[33].

Conseguentemente anche nel diritto civile, volgendo lo sguardo alle istituzioni giusprivatistiche, ed in particolare a talune categorie di diritti reali, come la proprietà, ci accorgiamo che i luoghi virtuali della rete – nel cui ambito è più agevole riscontrare negoziazioni aventi ad oggetto l'accesso e la riutilizzazione della proprietà piuttosto che la proprietà stessa[34] – sopravanzano le certezze granitiche di un diritto positivo che ha ancora bisogno di assolutezze, di fisicità (*iura in rem*) ovvero di un dove, in cui realizzare una funzione ordinatrice e manifestarsi come fenomeno di significazione culturale[35].

L'occasione di un ragionamento a tutto campo non può peraltro prescindere da un richiamo alle profonde trasformazioni che la rivoluzione digitale sta determinando anche nelle scienze penalistiche (si pensi ad esempio alle recenti modifiche inserite dalla l. 48/2008 nel c.p. in tema di reati informatici; ai temi della prova digitale nel processo penale ed alla *vexata quaestio* della compressione dei diritti fondamentali, provocata da taluni metodi investigativi ad alto contenuto tecnologico). Alla procedura penale, anzitutto, che vede vacillare i fondamenti del proprio statuto di accertamento fattuale, evidenziando rischi e pericoli a cui sono esposte talune garanzie di rilevanza primaria. Al diritto penale, costretto ad incalzare inedite forme di criminalità, sempre più globali e tecnologiche. Al diritto penale commerciale, obbligato a fronteggiare nuove forme di responsabilità societaria per fatti di reato legati al mondo di Internet ed infine alla criminologia, sospinta verso nuovi orizzonti di indagine, prospettati da una rete virtuale e senza perimetro o comunque dai contorni sempre più sbiaditi[36].

[33] Per un'approfondita disamina: L. LESSIG, *Remix, il futuro del copyright (e delle nuove generazioni)*, Firenze, Etas, 2009.

[34] La teoria è di J. RIFKIN, *L'era dell'accesso. La rivoluzione della new economy*, Milano, Mondatori, 2001.

[35] P. BARCELLONA, *Diritto privato e società moderna*, Napoli, Jovene, 1996, pp. 26 e ss.

[36] L. LUPARIA (a cura di), *Sistema Penale e Criminalità informatica,* Milano, Giuffrè, 2009, p. 9.

Sul tronco dell'astratta pretesa di un diritto adeguato all'evoluzione tecnologica, si innesta la versione futuribile ed efficientista di *giustizia* telematica prospettata, già nel 2001, nel primo regolamento per il processo civile telematico (Pct) e nelle sue successive rivisitazioni[37]. Il rapporto tecnologia e diritto è pronto ad invertirsi laddove l'informatica si mostra in grado di ricomporne i rigori procedurali, per assicurare la prioritaria necessità di ragionevole durata dei processi e, più in generale, per garantire ai cittadini un modello di giustizia civile fruibile anche se geneticamente modificata.

In tal senso sembrano orientate le prime sperimentazioni di *Polisweb,* la piattaforma di gestione telematica del processo civile, grazie alla quale, in taluni tribunali e solo per alcune tipologie di procedimenti[38], è diventato possibile per gli avvocati consultare, previa autenticazione con firma digitale e via *browser*, lo stato dei procedimenti (nomi delle parti, rinvii delle udienze, nomina dei giudici), inviare le comunicazioni fra le parti (al momento attiva solo per notifiche afferenti i procedimenti di ingiunzione) e redigere, direttamente in udienza, i verbali e in formato elettronico grazie a sofisticati software di *text to speech* (riconoscimento vocale). Nel breve termine, infine, irromperà nel processo civile telematico, anche la posta elettronica certificata (Pec), come previsto dal Dl 193/2009. Si gestiranno così, via Internet, anche le comunicazioni e le notifiche per gli avvocati, nell'auspicio di poter sviluppare infrastrutture e *software* – che oggi sono solo agli albori nel processo

[37] Il primo provvedimento in materia è il D.P.R. 13 febbraio 2001 n. 123 "Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della corte dei conti". La disciplina è stata successivamente rivisitata in d.m. 17 luglio 2008, recante "Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile", nonché nel d.m. 10 luglio 2009 rubricato "Adozione delle specifiche della strutturazione dei modelli informatici previste dall'art. 62, co. 2, del d.m. 17 luglio 2008".

[38] Il deposito telematico è attualmente attivo a valore legale per il procedimento di ingiunzione soltanto presso i seguenti 17 tribunali: Bergamo, Brescia, Catania, Genova, Busto Arsizio, Como, Lecco, Lodi, Milano, Monza, Pavia, Sondrio, Varese, Vigevano, Voghera, Napoli e Padova (*Rapporto di sintesi dicembre 2009 Servizi telematici giustizia civile*, a cura del Ministero della Giustizia, Dipartimento dell'organizzazione giudiziaria del personale e dei servizi, Direzione generale per i servizi informativi automatizzati).

civile e in uno stadio ancora più embrionale per quello penale – in grado di assicurare una più ampia base di effettività per la tenuta complessiva del sistema giustizia[39].

3. Innovazione 2.0 e nuova economia dell'informazione

Lungo questo tragitto di rinnovate consapevolezze e di nuovi dati di realtà, edificati da una digitalizzazione che muta le forme della regolazione giuridica, anche le certezze del processo economico, come il valore del capitale fisico – un tempo fondamento della civiltà industriale – iniziano ad incrinarsi e a vacillare. E da questo punto estremo, la contrazione del ciclo di vita dei prodotti consacra le logiche innovative di una rete che si limita a registrare, con disarmante naturalità, i riflessi edulcorati dell'anacronismo proprietario e lo sfaldamento dei paradigmi del possesso.

Assistiamo, così, alla nascita di nuovi archetipi (non solo *new economy* ma *networked economy,* economia informazionale e capitalismo digitale*)* e in ottica prospettica, diventiamo testimoni di una discontinuità storico-economica che sta consentendo all'informazione di diventare il prodotto di un processo produttivo[40].

Più in generale, gli schemi delle economie di condivisione e del capitalismo informazionale si sovrappongono, senza contrastarne le logiche, sia al capitalismo dello spazio e della materia sia ai tradizionali modelli economici commerciali[41].

In altri termini, il passaggio dall'industrialismo all'informazionalismo, pur non rappresentando l'equivalente storico del passaggio dall'economia agricola all'economia industriale, inizia a prospettare le dimensioni di un'agricoltura informazionale, di un'industria informazionale e di un terziario informazionale. Settori tutti che produrranno e distribuiranno sulla

[39] A. Longo*, Processo via Web*, in "Nova", Allegato al Sole 24 ore del 4.03.2010, p. 18.

[40] C. Freeman, *The Economics of Industrial Innovation*, London Pinter, 1997.

[41] "Un sistema economico disciplina quali cose vengono prodotte e con quali mezzi, chi le riceve e in cambio di quali prestazioni, e quale percentuale delle risorse sociali va destinata al risparmio ed alla fornitura di beni e servizi pubblici". Così J. Rawls, *Una teoria della giustizia*, Milano, Feltrinelli, 2008.

base di informazioni e conoscenze incorporate in processi di produzione globale, garantiti dalla diffusione di reti informatiche globali[42].

Il concetto stesso di catena del valore, in quest'ottica, viene sopravanzato da quello di rete del valore, ovvero dall'idea di una rete globale di aziende multimediali interconnesse e organizzate intorno a *partnership* strategiche[43]; da nuove forme di impresa cognitiva e collettiva, nonché da modelli economici ibridi caratterizzati da processi cooperativi ed oggetti condivisi, la cui valorizzazione dipende prevalentemente dai contributi partecipativi e di condivisione degli utenti[44].

Grazie alla crescente accessibilità delle tecnologie informatiche ed in particolare al *web 2.0*, le moderne imprese, ispirate dal paradigma dell'innovazione aperta o collaborativa, iniziano ad ideare, progettare ed erogare prodotti e servizi con modalità che non avevano precedenti nella storia[45]. Si cominciano ad allocare anche le attività di ricerca e sviluppo al di fuori dei confini dell'organizzazione aziendale. Si aprono i modelli di business a centinaia di milioni di persone, connesse all'ideagorà della rete, che collaborano per creare arte, scienza, economia, ricchezza e sviluppo sociale, o più semplicemente innovazione 2.0.[46]

Le aziende più lungimiranti, interagiscono sistematicamente con le *web-enabled community* ed hanno già aperto i loro processi produttivi all'ingegno collettivo, anche per poter competere con le *corporation* più ricche del mondo. Questo volto nuovo della normalità convive, di fatto, con l'attuale situazione di crisi economica ed è divenuto parte integrante di un'era della turbolenza. Uno stato di perpetua fibrillazione in cui, tanto i rischi quanto le opportunità, si fondono in un mondo interconnesso e caoticizzato, ai ritmi esponenziali della globalizzazione e dell'innovazione tecnologica[47].

[42] M. CASTELLS, *La nascita della società in rete*, cit., p. 107.

[43] M. CASTELLS, *Comunicazione e potere*, Milano, Egea, 2009, pp. 82 e ss.

[44] Così L. LESSIG, *op cit.*, pp. 137 e ss.

[45] S. NAMBISAN, *Transforming Government through Collaborative Innovation*, Innovation Series, IBM Center for the business of government.

[46] H. CHESBROUGH, *OPEN, Modelli di Business per l'innovazione*, Milano, Egea, 2008, p. 40.

[47] P. KOTLER, J.A. CASLIONE, *Chaotics. Gestione e marketing nell'era della turbolenza*, Torino, Sperling & Kupler, 2009, pp. 12 e ss.

Le nuove infrastrutture collaborative a basso costo – dai *software open sources,* alle piattaforme globali promosse dai mercati secondari dell'innovazione – hanno così consentito alle prime *start-up* di diventare co-creatrici e co-produttrici di beni o servizi su larga scala, con modalità che in precedenza potevano essere garantite solo dalle grandi multinazionali.

In tale quadro, l'attribuzione tipica di ogni forma di innovazione 2.0 assume la denominazione di *peer production*[48], ossia di quel fenomeno che si realizza quando una massa di persone o di aziende concorrono con un approccio "aperto" a promuovere l'innovazione (in questo specifico caso si ricorre anche alla definizione di *Network Centric Innovation*)[49] e la crescita del proprio settore di appartenenza.

La collaborazione di massa e l'architettura della partecipazione promossa dalla rete, stanno quindi emergendo come nuovo fenomeno economico (*wikinomics* o economia collaborativa*)* ed imprenditoriale (*network enterprise*), basato sui concetti di apertura, condivisione radicale, *peering* e azione globale[50]. Tutto ciò in aperta discontinuità con regole consolidate e dogmi di *business administration* che vivevano fino a qualche anno fa, ai confini dell'anonimato, in tutte quelle divisioni aziendali affette dalla sindrome del *not invented here (NIH)* e dal virus del *not sold here (NSH)*[51].

Alla stregua dei modelli partecipativi descritti, ogni singolo individuo avrà un ruolo da svolgere nell'economia, ed ogni impresa, di conseguenza, disporrà della stessa opzione di scelta: scivolare nell'anonimato o connettersi al resto del mondo[52].

[48] Collaborazione di massa o produzione ad opera di un gruppo di pari. Il termine è stato coniato da YOCHAI BENKLER, *Coase's Pinguin or Linux and the Nature of the Firm*, in "Yale Law Journal", Vol. 112, 2002-2003.

[49] Per un'ampia trattazione del tema: S. NAMBISAN, M. SAWNEY, *The Global Brain*, Wharton School Publishing, 2008.

[50] D. TAPSCOTT e A. D. WILLIAMS, *Wikinomics*, Milano, Etas 2008, p. 29.

[51] La sindrome NIH si basa in parte su una sorta di xenofobia: non possiamo fidarci perché non viene dall'interno dell'azienda e quindi differisce dal nostro modo di operare. Il virus NSH induce invece ad affermare che se non vendiamo una certa cosa non dovrebbe venderla nessun'altro. Così H. CHESBROUGH, *op. cit.*, pp. 26-39.

[52] D. TAPSCOTT, A. D. WILLIAMS, *op. cit.* p. 29.

4. Innovazione infrastrutturale fra regolamentazione e mercato

Da tali premesse, che stanno rivoluzionando i processi di circolazione della conoscenza, del potere e del capitale, nasce un'importante e per alcuni versi rivoluzionaria sfida per il mondo delle telecomunicazioni.

Il ritmo del cambiamento sociale, scandito dalla propagazione delle reti virtuali e infrastrutturali di ultima generazione (*Next Generation Network*)[53] sta infatti delineando un nuovo orizzonte di civiltà, per tutto il sistema paese, identificato proprio nella *digital prosperity*.

Un'ondata di innovazione tecnologica e di mercato, all'interno della quale dovrà essere coniugata la domanda di servizi a banda larga per l'accesso ad Internet (da postazioni fisse e mobili) con la necessità degli operatori di far fronte agli ingenti investimenti necessari alla realizzazione delle reti in fibra ottica (*Broadband*) e delle reti di nuova generazione (*Ultrabroadband*).

In tale quadro, la possibilità per gli *incumbent,* proprietari o gestori delle reti infrastrutturali, di incrementare la capacità trasmissiva, per governare la transizione verso il mondo *All IP,* non potrà certamente essere concepita come condizione di sviluppo della rete fisica, imputabile in via esclusiva al sistema impresa.

L'innovazione infrastrutturale rappresenta, infatti, una variabile dipendente anche dalle scelte finanziarie dello Stato in cui si realizza. In essa convivono il diritto della concorrenza, l'opzione regolatoria prescelta al fine di favorire il mercato delle comunicazioni elettroniche (*wholesale e retail*) e le garanzie dei diritti inderogabili di libertà delle persone, nonché del diritto di iniziativa economica, in regime di libera concorrenza.

In tale scenario, la condizione primigenia e ottimale, per la creazione effettiva di un mercato *pro-concorrenziale,* sarebbe in astratto rinvenibile nella possibile realizzazione di diverse infrastrutture di rete concorrenti, attraverso cui fornire altrettanti servizi in concorrenza.

La strada della replicabilità infrastrutturale tuttavia, per una molteplicità di ragioni (*in primis* di convenienza economica), non è sempre percorribile. Pertanto in situazioni di *ladder of investments* – in cui si rendono necessari interventi rimediali finalizzati ad evitare l'abuso di posizioni

[53] La realizzazione della NGN determinerà la migrazione di tutto il traffico voce su rete IP garantendo la connessione a banda larga *(broadband)* a tutto il paese entro il 2012.

dominanti e ad assicurare *l'uso delle reti a condizioni oggettive, trasparenti e non discriminatorie* – la parità delle condizioni di accesso e interconnessione deve essere garantita da organi statali sovraordinati (*ex post* in applicazione del diritto della concorrenza ed *ex ante* con l'attuazione di disposizioni regolamentari) anche mediante la scelta di modelli separazione funzionale[54], strutturale[55] o intermedia della rete[56].

Al quadro delle possibili soluzioni attuabili, si va tuttavia accostando un nuovo scenario in grado di porre seriamente in discussione il paradigma della centralità della rete come infrastruttura. In altri termini, le grandi aziende del *web* stanno velocemente dispiegando ai bordi della rete (*edges*) enormi *data center*, costituiti da centinaia di migliaia di nodi di computazione, organizzati in sistemi di *server* interoperanti *(cloud computing*), in grado di alimentare le potenti piattaforme utilizzate per fornire i servizi *web 2.0*.

Le conseguenze di questo spostamento di intelligenza rischiano di diventare deleterie per gli operatori di TLC, depauperati dei ricavi derivanti dai ricchi e costosi servizi di funzionalità di rete (c.d. *Value added services* o semplicemente servizi VAS), non più utilizzati da utenti finali pronti ad avvalersi di quelli forniti ai bordi della rete, da cui parte una nuova catena *(rectius rete)* del valore svincolata dagli obblighi regolatori.

Nel lungo periodo gli operatori potrebbero pertanto essere confinati al ruolo di meri fornitori di connettività (*Bit Pipe Provider*), lasciando il mercato dei servizi alle *Web Company*, con preoccupanti ripercussioni sull'industria tradizionale delle telecomunicazioni e sulla complessiva tenuta della concorrenza e del mercato[57].

La soluzione richiesta per evitare il collasso del sistema – avallata anche dalla più qualificata dottrina – oltre alla tradizionale formula del finanziamento statale alle infrastrutture, potrebbe consistere nel considerare l'obiettivo di promuovere l'innovazione della rete come condizione

[54] Modello *Openreach* adottato per British Telecom nel Regno Unito.

[55] Modello adottato nel 1982 da AT&T negli Stati Uniti.

[56] Modello adottato in Italia, con grande apprezzamento espresso in ambito nazionale e comunitario, con il modello *Open Access* proposto da Telecom Italia e successivamente ratificato dall'Autorità Garante per le Comunicazioni.

[57] R. MINERVA, *I paradossi della rete: come sopravvivere in un oceano rosso e sognare un oceano blu*, in "Notiziario Tecnico Telecom", anno 18, n. 3, 2009, pp. 54 e ss.

di *public policy* e quindi di sviluppo del sistema paese e contestualizzare, in tali ipotesi, la possibilità di *regulatory holidays* che sospendano i più stringenti vincoli regolamentari per gli *incumbent* impegnati nello sviluppo e nell'innovazione strutturale della rete[58].

La sospensione di taluni obblighi regolatori – come *extrema ratio* a cui ricorrere in presenza di situazioni di grave crisi del modello economico, corroborate da una situazione di insufficienza infrastrutturale – sarebbe comunque giustificata da un superiore interesse pubblico generale alla fornitura di servizi universali[59], nonché dalla necessità di ritenere preminenti i risultati di efficienza dinamica rispetto a quelli di efficienza allocativa[60].

Le implicazioni riguardanti le strategie di sviluppo delle reti di comunicazione elettronica, in funzione delle moderne variabili tecnologiche, colgono pertanto un ulteriore aspetto di centrale rilevanza nella nostra analisi, ovvero quello della necessità di adottare modelli di *business* sostenibili, in presenza di piattaforme già affermate e di *community* composte da milioni di persone abituate a vivere relazioni *on-line,* in una piazza virtuale, popolata e famigliare[61].

Non esistono soluzioni univoche, ma la gestione proprietaria delle piattaforme, coniugata con l'etero-regolamentazione del *web 2.0*, rappresenta oggi il sistema ibrido, più flessibile e riuscito di *engagement* fra community e aziende di servizi di comunicazione elettronica, accessibili al pubblico della fruizione *pull* dei contenuti[62].

Nello specifico, il modello di autocomunicazione di massa[63] con maggiori opportunità di affermazione sembra essere quello sviluppato all'interno delle infrastrutture di servizio, dove anche se l'apertura sugli utenti

[58] P. CONGEDO, *Structural or Functional Separation in Regulated Industries? Winners Do Not Punish; Possibly Cooperate*, MPRA, 2008, pp. 15 e ss.

[59] Vi è ormai ampio consenso nel riconoscere alla banda larga il ruolo di servizio primario ed i principali Paesi europei, inclusa l'Italia, stanno cercando di garantire il servizio universale *de facto* ad almeno 2Mbit/s a tutta la popolazione.

[60] G. MONTI, *Managing the Intersection of Utilities Regulation and EC Competition Law*, in "The Competition Law review", Vol. 4, n. 2, 2008, pp. 128 e ss.

[61] *Open Mind, Il web 2.0 e le sue conseguenze sull'impresa,* Roma, Elibri, Telecom Italia, 2009, pp. 5 e ss.

[62] Il pubblico sceglie i contenuti anziché subirli passivamente.

[63] M. CASTELLS *Comunicazione e potere*, cit., pp. 64-81 e ss.

e sulle metriche è totale (ad es. Facebook, Twitter o motori di ricerca come Google oppure NETtv come Youtube) viene comunque mantenuto il controllo di due profili. Il primo è quello delle modalità di caratterizzazione delle nuove piattaforme, con funzionalità e servizi tali da non rendere replicabili le loro esperienze al di fuori dell'ambiente virtuale proposto; il secondo è quello del consolidamento di standard di interoperabilità per lo sviluppo di applicazioni (*killer application*) da usare soprattutto nel *network* (come ad esempio i contenuti innovativi veicolati da *widget* multimediali e *feed RSS*). Attraverso queste ultime modalità si sviluppa l'interesse dell'utente ad entrare in una *community* o comunque in un ambiente virtuale ed a rimanerci fino a diventarne parte attiva e generatrice di contenuti. La via della partecipazione ha pertanto trasformato l'utente in modo radicale, da semplice consumatore in *prosumer*[64], ossia in utente/consumatore/autore/produttore, che attraverso un processo di *User Generated Content* (USG), assume la possibilità di far convergere informazioni e contenuti, precedentemente aggregati, in un unico *media* capace di far arrivare ad una comunità di riferimento la condivisione finale di taluni dati. L'idea assume una portata rivoluzionaria nel momento in cui tali dati si trasformano in *input* precisi in grado di innovare prodotti o servizi (in una sorta di continuo scambio fra aziende e utenti che creano ricerca e sviluppo) e di riconfigurarne i rispettivi cicli di durata.

La diffusione di modelli di business che incoraggiano i clienti a sviluppare innovazione sostenibile, decreterà così la fine dei processi di produzione statica, destinandoli a degna sepoltura nella grande discarica della storia.

5. Internet e cyberdemocrazia

La creazione di una rete con contenuti di valore rinvia, infine, all'esistenza di un nesso di compenetrazione più profondo con l'utente. Una relazione che oggi si esprime in termini di *net neutrality* e di *Internet trustworthiness* ed è volta ad acquisire fiducia ed a promuovere garanzie e principî di democrazia e libertà attraverso la rete[65].

[64] Termine coniato da A. Toffler in *La terza ondata,* Milano, Sperling & Kupfer, 1987.

[65] Non esiste una singola definizione comunemente accettata di *Net Neutrality*. Si tratta di un'espressione coniata negli Stati Uniti alla quale sono stati poi associati una serie di

"La nostra comunità rappresenta un'opportunità per osservare le regole che governano la società e, per quanto ci è concesso, di riscriverle nel modo che sembra più adatto a noi". Sono le parole che Philip Rosedale (fondatore di Linden Lab, società californiana che ha sviluppato *Second Life)* ha recentemente rivolto ad una platea virtuale riunita *on-line* in un anfiteatro costruito su *Second Life,* per la presentazione di un libro del Professor Lawrence Lessig (docente presso la facoltà di giurisprudenza dell'Università di Stanford). Le guarentigie partecipative di un'agorà virtuale*,* cumulativa e non sostituiva della piazza reale, a cui faceva riferimento Rosedale, razionalizzano la base d'azione cognitiva di una società civile, consapevole e plurale, ove il cittadino digitale, contribuisce anche alla creazione delle condizioni per il legittimo esercizio dei pubblici poteri. Ciò accade, soprattutto laddove la rappresentazione del potere in rete avviene in un dibattito sulla sfera pubblica, in cui gli utenti finali intervengono con spirito critico e con la possibilità di integrare, e persino di rettificare, i contenuti espressi dalle *corporation* delle comunicazioni. Il *web* assume, in tale particolare ambito, la connotazione di una rete di fiducia, in quanto i suoi contenuti suscitano empatia nell'elaborazione mentale dei messaggi degli utenti, attraverso i quali nascono le moderne forme di autocomunicazione di massa e di mobilitazione sociale, tipiche della *Network Centric Advocacy*[66].

comportamenti ritenuti anticompetitivi o comunque lesivi degli interessi della collettività. In generale il rispetto del principio della *Net Neutrality*, nel senso più restrittivo del termine, richiede che il traffico internet sia trattato dalla rete nello stesso modo senza discriminare o agevolare determinati flussi (pacchetti di traffico IP) rispetto ad altri. Tuttavia, la possibilità per l'operatore di rete, di fornire un servizio diverso (rispetto ad una pluralità di parametri, quali banda, latenza, *packet loss*, *bitter*, etc., definito "network management") permette di estrapolare parte del surplus del fornitore di contenuti e/o, del consumatore, attraverso un *pricing* differenziato per tipologia di servizio. Il dibattito sulla *Net Neutrality* è nato dal timore che tale comportamento da parte degli operatori di rete possa creare un'eccessiva penalizzazione per i livelli di servizio più economici, di fatto, limitando la libera circolazione di contenuti e di idee che caratterizza la rete Internet. La potenziale discriminazione tra fornitori di contenuti, in base alla capacità/volontà di "acquistare" servizi di maggiore qualità, potrebbe, secondo i promotori della *Net Neutrality*, orientare la comunicazione.

[66] Il fenomeno riguarda i gruppi di difesa sociale i quali si sono resi conto che i principî base della *Network Centricity* possono essere adottati per coinvolgere in tempi strettissimi un gran numero di persone e scalare velocemente le competenze, le risorse, il sostegno pubblico e le informazioni per rendere matura una campagna di rivendicazioni sociali.

La proliferazione delle reti di comunicazione, nelle sue varie forme, (virtuale, infrastrutturale e istituzionale[67]) ha così contribuito all'affermazione di movimenti spontanei di rivendicazione sociopolitica che hanno consolidato una nuova autonomia rispetto ai governi ed ai *media* tradizionali. In numerose nazioni, ad esempio, manifestanti e attivisti, potenziati da dispositivi che dotano di connettività perpetua, hanno usato la loro capacità comunicativa per amplificare l'impatto delle proteste sociali, estendendolo in tutto il mondo (come avvenuto nelle recenti elezioni Iraniane)[68].

Sotto quest'ultimo profilo, pertanto, può ritenersi trasposta un'ulteriore forma di garanzia di espressione effettiva delle idee e delle opinioni difformi da quelle maggiormente condivise all'interno di un corpo sociale, normativamente inclusa nei contenuti precettivi degli articoli 2 e 21 della Costituzione[69].

Questa visione eclettica della rete va, pertanto, al di là della funzione strumentale di coordinare le azioni e sfruttare la flessibilità dei *networking* di movimento e degli *insurgent politics*, e si fa altresì garante del superamento del tradizionale schema *top down* di "opinione pubblica avvertita".

L'osservazione dell'attivismo politico *on-line* dimostra, inoltre, come Internet rappresenti la condizione primigenia per lo sviluppo delle agorà virtuali, ossia di quelle comunità virtuali *pluripartisan* dedicate all'opinione politica, il cui principale obiettivo è dato dall'assistenza al dialogo, alla delibera, alla decisione e all'azione di tutti i cittadini che desiderino parteciparvi[70].

Ne deriva un fondamentale contributo, espresso dalla rete in termini di effettività, alla coproduzione di significati valoriali, complementari al pro-

[67] In tal senso F. DI PORTO, *La disciplina delle reti nel diritto dell'economia*, Padova, Cedam, 2008.

[68] M. CASTELLS, *Comunicazione e potere*, cit., p. 437.

[69] R. MESSINETTI, *op. cit.,* p. 19.

[70] P. LEVY, *Cyberdemocrazia.* cit., p. 160. Secondo Levy questa finalità può essere raggiunta attraverso tre modalità: "In primo luogo strutturando il dialogo collettivo in problemi e non in partiti; solo in un secondo momento, in posizioni e tipi di argomentazioni; in secondo luogo mettendo a disposizione dei partecipanti, l'insieme delle informazioni pertinenti, accessibili attraverso dei semplici *link* ipertestuali; in terzo luogo, mettendo a disposizione degli utenti gli esperti nell'organizzazione (creazione *ad hoc* di *forum* su determinati argomenti, strumenti di aiuto per la coordinazione), d'espressione, d'azione (petizioni ecc.) e di consulta (voto elettronico, sondaggi ecc.)".

cesso di partecipazione democratica alla vita delle istituzioni di un paese. Anzi, in un approccio più costruttivo all'interpretazione di un processo di evoluzione sociale, si potrebbe concettualizzare proprio quella "nuova forma di società in rete", teorizzata da Manuel Castells e costituita da specifiche configurazioni di reti globali, nazionali e locali, in uno spazio multidimensionale di interazione sociale. Una nuova società, i cui confini sarebbero altamente instabili, per l'incessante mutamento nella geometria delle reti globali che strutturano le pratiche e le organizzazioni sociali[71].

6. Innovazione collaborativa ed organizzazioni eterarchiche

Per concludere, anche nei contesti strutturati e sistemici delle organizzazioni istituzionali e aziendali e nell'ambito dei modelli di gestione delle risorse umane, il fenomeno rete inizia ad esprimere un valore determinante. Si evidenzia cioè un'architettura della partecipazione proposta da Internet – aperta, piatta e flessibile – che sta incominciando a rappresentare un modello di relazione in cui riflettere nuove teorie di management 2.0. o di organizzazione post-manageriale[72]. Ed infatti, nell'ultimo secolo, si è a lungo dibattuto sulla supposizione che le persone non fossero in grado di organizzarsi autonomamente. La scelta tra mercato e pianificazione dava per scontato che non esistesse una terza via. Ora quella via esiste e la facilità di coordinamento e di azione collettiva, propria del paradigma dell'innovazione aperta o collaborativa, la sta scoprendo attraverso l'indebolimento delle tradizionali forme di organizzazione istituzionale e gerarchizzata.

Le reti informatiche abilitano a nuove forme di organizzazione eterarchica, di dimensioni inimmaginabili rispetto al passato, con ciò determinando un esponenziale abbassamento dei costi di transazione (o coordinamento). Nello specifico, se è vero – come teorizzato dall'economista Ronald Coase – che un'organizzazione tende a crescere solo nel momento in cui i vantaggi derivanti dalla gestione di un maggior numero di impiegati dovessero essere maggiori dei costi di transazione necessari a gestirli, cosa dovrebbe accadere a tutte quelle attività di gestione e orga-

[71] M. Castells, *Comunicazione e potere*, cit., pp. 13 e ss.

[72] C. Shirky, *Uno per uno, tutti per tutti,* Torino, Codice, 2009, pp. 34-42.

nizzazione non comparabili con i costi manageriali[73]? Fino a qualche tempo fa la risposta sarebbe stata semplice, in quanto non sarebbero state prese in alcuna considerazione dalle organizzazioni aziendali statiche. Oggi, di contro, la possibilità di attuarle si è manifestata concretamente grazie all'abbassamento dei costi di transazione, assicurato dalle dinamiche partecipative generate dai modelli di collaborazione di massa, attuati grazie alle reti di comunicazione elettronica.

I modelli organizzativi centrati sul controllo e l'efficienza, in sostanza, non sembrano più sufficienti a competere in un mondo in cui l'adattabilità e la creatività diventano il regime motore del successo e del vantaggio competitivo ed i costi delle attività di condivisione, collaborazione e azione collettiva sono scesi significativamente.

La rete, in sintesi, sta offrendo al mondo un nuovo strumento sociale: l'azione di gruppi poco strutturati, che operano senza direzione manageriale, al di fuori delle logiche gerarchiche o di organizzazione istituzionale. Una nuova forma di autopoiesi organizzativa, intesa, appunto come capacità di organizzazione autonoma e di mantenimento costante ed efficace della strutturazione interna di un sistema sociale[74].

L'innovazione autentica, inizialmente connaturale ai prodotti, ai processi o alle strategie, privilegio esclusivo dei patriarchi dell'organizzazione, inizia allora a concretizzarsi anche in un altro aspetto, ossia nella forza del *web* di dar voce al contraente debole (consumatore, lavoratore subordinato o più semplicemente utente o fruitore) e cancellare schemi negoziali fumosi e inutili spesso consolidati nel tempo.

La rete ormai non si ferma alle persone, ai gruppi, agli Stati, alle comunità internazionali. Si rivolge all'umanità intera ed attraverso quest'ultima lancia l'attacco finale ai modelli di *management* del passato ed alle gerarchie paralizzanti, distribuite secondo flussi monodirezionali di comando e controllo. La vicenda dell'ultima ora si trasforma così in un augurio di speranza: affinché nell'era digitale l'unico modo per costruire una società in grado di affrontare il futuro, diventi quello di crearne una in linea con

[73] R.H. COASE, *The Nature of the Firm*, IN "Economica", 1937, pp. 386-405.

[74] *Autos* =se e *Poiesis* = creazione, sul tema si veda l'ampia trattazione di H.R. MATURANA, J. VARELA, *Autopoiesis and Cognition: the Realization of the Living*, Amsterdam, Kluwer, 1980.

le esigenze degli esseri umani[75]. Una dimensione in grado di promuovere e sostenere l'iniziativa, la creatività, le aspettative e la passione delle persone sfruttando la capacità del *web* di riconoscerle e regolamentarsi come luogo di insediamento di diritti e responsabilità.

[75] G. HAMEL, *Il futuro del management*, Harvard, Harvard Business School Press, 2008, p. 175.

I rischi del diritto nella Rete globale

GIOVANNI PELLERINO*

SOMMARIO: *1. Diritto "nella Rete" – 2. Il sistema giuridico e il suo paradosso – 3. Il diritto dei naviganti – 4. Possibilità e limiti del diritto nell'età tecnologica*

1. DIRITTO "NELLA RETE"

La riflessione teorico-giuridica dell'ultimo decennio del secolo scorso si è caratterizzata per un ritorno ai diritti fondamentali. Come è noto, fu Bobbio ad inaugurare quella stagione che egli stesso designò come "Età dei diritti"[1].

Il Novecento si chiudeva con il crollo dei regimi dell'Est e l'apertura di nuovi spazi di democrazia richiedeva al diritto di affermare con rinnovato vigore i principî di legalità. In questo contesto, diventava cruciale la questione dei diritti fondamentali; non il problema della giustificazione del loro fondamento, bensì la ricerca delle modalità più efficaci per declinare la loro concreta attuazione[2]. La storia del costituzionalismo moderno, infatti, aveva dimostrato che, al riconoscimento sempre più ampio della titolarità formale di nuovi diritti, era corrisposta una effettività decrescente del loro godimento.

I diritti fondamentali dovevano essere intesi non come diritti eterni, connaturati all'uomo, ma come diritti storici, nati nella realtà sociale dalle lotte dei popoli nei confronti dei dogmatismi delle religioni e degli autoritarismi degli Stati nazionali.

In una prospettiva evolutiva, sarebbe possibile distinguere quattro generazioni di diritti fondamentali: una prima, in cui si sono affermati i diritti individuali, le libertà illuministiche reclamate dalla borghesia e proclamate con le Rivoluzioni americana e francese (libertà nello Stato); una seconda, in cui sono stati conquistati i diritti sociali, nella quale lo Stato deve svolgere una parte attiva, al fine di costruire le condizioni o rimuo-

* L'Autore è professore aggregato di Informatica giuridica presso la Facoltà di Giurisprudenza dell'Università del Salento (giovanni.pellerino@unisalento.it).

[1] N. BOBBIO, *L'età dei diritti*, Torino, Einaudi, 1990.

[2] Cfr. S. RODOTÀ, *Repertorio di fine secolo*, Roma-Bari, Laterza, 1992.

vere gli impedimenti per la loro garanzia (libertà per mezzo dello Stato); una terza, in cui sono stati riconosciuti i diritti individuali e sociali non solo ai singoli, ma ai gruppi umani e ai cittadini del mondo (ambiente, salute, pace); una quarta, in cui si ricomprendono, tra gli altri, quei diritti legati allo sviluppo delle nuove tecnologie, in particolare dell'informatica e delle telecomunicazioni (privacy, sicurezza, accessibilità).

A ben vedere, un *fil rouge* mette in relazione i diritti di libertà della prima generazione con quelli dell'ultima e stabilisce un legame di continuità che non è solo di carattere cronologico. Infatti, così come le prime libertà poterono affermarsi, a livello costituzionale, nelle temperie politico istituzionali che seguirono le due rivoluzioni industriali della metà del Seicento e dell'inizio dell'Ottocento, così i diritti di ultima generazione sono diretta conseguenza di quel passaggio evolutivo di portata epocale, non dissimile da ciò che si era prodotto per effetto della rivoluzione industriale, rappresentato dall'avvento di Internet.

Di fronte a questa rivoluzione tecnologica, che ha segnato il passaggio dal vecchio al nuovo Millennio[3], il diritto, come vedremo, ha tentato, in una prima fase, di adattarsi utilizzando i presupposti teorici e i luoghi argomentativi di cui disponeva. La comunicazione giuridica ha inizialmente ignorato il fenomeno e, solo successivamente, ha rincorso le innovazioni che si producevano nel *ciberspazio*, tentando di "addomesticarle" all'interno di istituti già esistenti, spesso senza coglierne in pieno le specifiche peculiarità.

È così accaduto che, in alcuni casi, il diritto abbia utilizzato norme per certi aspetti obsolete, come la legge italiana sul diritto d'autore, per tutelare la proprietà intellettuale in Internet; ovvero, in altri casi, abbia abdicato alla regolazione di aspetti fondamentali quali, ad esempio, quelli legati alla *governance* della Rete.

Il corto circuito che ha investito il diritto di fronte a queste problematiche deriva innanzitutto dalla natura che esso ha assunto fin dagli albori della modernità; con la nascita degli Stati nazionali, il diritto ha perso il suo carattere universalistico e si è abituato ad operare nell'am-

[3] La sensibilità collettiva fu segnata a tal punto, che la semantica sulla fine del mondo, la quale si alimenta in maniera ricorrente ai passaggi millenari, si arricchì di una nuova locuzione relativa alla Rete: il *Millennium bug*.

bito ristretto dei singoli ordinamenti. Se si eccettuano le norme del diritto internazionale (pubblico e privato), che occupano uno spazio limitato rispetto alla mole dei diritti nazionali, occorre riflettere sul fatto che il diritto moderno si è riprodotto nel segno della pluralità e non dell'unità. All'antico particolarismo giuridico che si caratterizzava per le differenze di ceti e di *status*, è succeduto un nuovo particolarismo di natura politico-territoriale[4].

La tesi che in questa sede si intende sostenere, è che l'avvento della Rete abbia dato inizio ad un lento ma inesorabile processo di disgregazione delle fondamenta stesse del sistema giuridico contemporaneo. Il "diritto della Rete" può rischiare di far cadere il "diritto nella Rete", può rischiare, in altri termini, di rendere palesi le contraddizioni e i limiti costitutivi del diritto, rendendolo altamente vulnerabile.

Nella prospettiva del diritto pubblico, il livello dei rapporti tra governanti e governati viene modificato da uno strumento che permette una circolazione notevolmente più accentuata delle informazioni e della conoscenza, consentendo un significativo incremento dei meccanismi di controllo sui governanti; a tali condizioni, il grado di libertà dei cittadini tende ad aumentare in maniera inversamente proporzionale rispetto alla pressione del potere politico. Internet rappresenta uno strumento di accrescimento delle conoscenze e della libertà, portando con sé un ampliamento degli strumenti di governo non autoritativi e consensuali cui corrisponde una riduzione di quelli di tipo autoritativo. Inoltre, lo stesso sistema delle fonti viene modificato. Nel costituzionalismo moderno, le fonti sono tradizionalmente di origine statale, a partire dalla legge; ebbene, la Rete favorisce fenomeni di destatualizzazione delle fonti in due direzioni opposte: da un lato, accrescendo il ruolo delle fonti di livello internazionale; dall'altro, incentivando le fonti che derivano dall'autoregolamentazione. Infine, la diffusione dell'accesso a Internet incide profondamente sui contenuti dei diritti fondamentali. Dei diritti di partecipazione politica abbiamo appena detto; quanto alle libertà economiche, è possibile osservare l'accentuazione di quel processo che porta a ridimen-

[4] F. GALGANO, *I caratteri della giuridicità nell'era della globalizzazione*, in "Sociologia del diritto", n. 1, 2003, p. 10.

sionare gli spazi del diritto di proprietà, inteso in senso tradizionale, nonché ad incrementare la libertà di iniziativa economica e la concorrenza; in relazione alla libertà di comunicazione, occorre notare che si assiste ad una profonda rimodulazione dello statuto di questa libertà, con riferimento da un lato alle nuove problematiche che investono la *privacy* (le tecnologie elettroniche hanno introdotto un nuovo modo di costruzione della sfera privata, con la possibilità di organizzare, unificare e far permanere informazioni disperse o destinate a scomparire) e dall'altro al sostanziale accorpamento di diritti che nella tradizione europea erano stati tenuti separati (libertà di manifestazione del pensiero, libertà di espressione, libertà di corrispondenza, libertà di ricevere e trasmettere informazioni).

Nella prospettiva del diritto privato, la dottrina ha iniziato a domandarsi quale futuro possa esso avere all'interno del "villaggio globale" di una società che ha dimensioni planetarie. L'ambito di applicazione del diritto civile, apparentemente, si dilata a dismisura in rapporto all'espansione dei rapporti giuridici nel mercato globale, sia che essi intercorrano tra imprese sia tra imprese e consumatori. Si pensi al contratto *on line*, un negozio concluso fuori dallo spazio; il problema è che nessun ordinamento nazionale risulta applicabile sulla base delle tradizionali regole del diritto internazionale privato. Qualcuno ha addirittura concluso che si tratterebbe di un contratto collocabile fuori dal diritto[5].

La realtà è che gli ordinamenti nazionali risultano insufficienti a cogliere la dimensione della questione. Il problema investe i fondamenti stessi del sistema giuridico.

2. Il sistema giuridico e il suo paradosso

Pare opportuno domandarsi, a questo punto, quali siano, in termini sistemici, la struttura e la funzione del diritto nella modernità, tentando di disvelare il suo paradosso costitutivo.

Muovendo da questo obiettivo, si tenterà di operare una osservazione di secondo ordine, utilizzando le più recenti acquisizioni della Teoria della società[6].

[5] Ivi, p. 13.

[6] Cfr. N. Luhmann, R. De Giorgi, *Teoria della società*, Milano, F. Angeli, 1992.

In questa prospettiva è possibile riflettere sul fatto che il diritto può essere rappresentato come un sottosistema della società moderna, la cui funzione è quella di mantenere stabili delle aspettative anche nel caso in cui esse vengano deluse. Tali aspettative sono norme che restano stabili indipendentemente dalla loro violazione.

A partire dal secolo XVII, il sistema giuridico si differenzia quale sottosistema della società moderna, che svolge le funzioni di generalizzazione e stabilizzazione delle aspettative di comportamento. I suoi elementi sono tutte le comunicazioni sociali formulate in relazione al diritto: sia che esse siano svolte nell'ambito di procedimenti giuridici, sia che vengano espresse nella vita quotidiana[7]. Nel corso di questo processo, il diritto da un lato si autonomizza rispetto agli altri ambiti della società e dall'altro si autolegittima attraverso la piena positivizzazione. Non occorre più, come era avvenuto fino al giusnaturalismo, rinvenire la fonte di legittimazione del diritto nella "verità" o, comunque, in istanze esterne al sistema. Il diritto è valido semplicemente perché è posto, vale a dire in quanto è il prodotto di una decisione. In altri termini, il diritto si fonda sul paradosso della sua contingenza: è valido oggi un diritto che domani potrà non essere più valido. È proprio il carattere della contingenza, l'istituzionalizzazione della possibilità di mutamento attraverso la legislazione, che consente al diritto moderno di incrementare la propria capacità di selettività ed elaborare un livello crescente di complessità. Questo non significa che tutto il diritto possa essere mutato a piacimento da diritto diverso: nell'ambito della comunicazione giuridica solo uno spazio limitato è riservato alla legislazione. Una variabilità troppo elevata delle informazioni renderebbe impossibile la comprensione e creerebbe un *impasse* comunicativo all'interno del sistema. È a questo scopo che viene mantenuta una semantica fondata sulla tradizione che si sedimenta nel corso del tempo in quelle astrazioni giuridiche conosciute come istituti.

Per il sistema del diritto, l'evoluzione semantica è stata meno appariscente rispetto ad altri ambiti di funzioni, in quanto, all'inizio dell'età moderna, esso poteva già contare su un alto grado di differenziazione sia della concettualità, sia degli apparati istituzionali. Tuttavia, è possibile

[7] N. LUHMANN, *La differenziazione del diritto*, Bologna, Il Mulino, 1990.

osservare come concetti fondamentali come quelli di diritto naturale, diritto positivo, proprietà, abbiano assunto un significato completamente nuovo, così come sono sorti neologismi per indicare rimandi di senso che in precedenza non esistevano (diritto amministrativo, diritto fondamentale, informatica giuridica e così via …)[8]. È proprio questo carattere del diritto a rendere più lento il suo processo di adattamento alle "irritazioni" che provengono dall'ambiente.

All'interno del sistema giuridico, il diritto dell'informatica che, in questa sede, ci riguarda più da vicino, rappresenta uno di quelli che vengono definiti "nuovi diritti", diritti di generazione successiva rispetto agli altri che si sono consolidati nel corso dei secoli.

Si tratta di un diritto nato nella modernità per venire incontro alle esigenze di regolazione di situazioni e soluzione di problemi che, prima dell'avvento delle nuove tecnologie, non erano neppure immaginabili. Non si deve credere, tuttavia, che regolare e normativizzare un nuovo ambito dell'agire sociale possa significare minimizzare i rischi di commissione di illeciti. Quello che si verifica è, semplicemente, una dislocazione del problema.

Questa circolarità che scaturisce essenzialmente dal fatto che le situazioni di rischio non si lasciano raffigurare come situazioni problematiche di tipo normativo, costringe il diritto a pratiche di applicazione pattuita del diritto stesso, conferisce al giudice, da una parte, al soggetto del diritto, dall'altra, un potere di contrattazione che estende continuamente i margini di tolleranza dell'illecito.

Il diritto fornisce sempre meno garanzia contro le delusioni, mentre lo stesso accesso al diritto diventa un accesso rischioso.

Il codice che orienta il diritto è costituito dalla differenza binaria ragione/torto: si ha comunicazione giuridica ogni volta che, in caso di controversie, qualcuno rivendichi dei diritti e, in ragione della normativa vigente, si deve giungere a decidere chi ha ragione e chi ha torto. Il diritto, dunque, è un sistema che risolve i conflitti ma, allo stesso tempo, ne genera anche, poiché sulla base del diritto si può resistere a delle pressioni o si possono generare nuovi contenziosi.

[8] G. PELLERINO, *L'idea di proprietà. Storia come evoluzione*, Lecce, PensaMultimedia, 2004.

Le norme giuridiche garantiscono una delimitazione di ciò che ci si può aspettare in futuro e, in questo senso, limitano la libertà e discriminano tra ciò che è accettabile e ciò che non lo è: con la normazione la società cerca di rendere gestibile un futuro che è in sé insicuro.

Questo vincolo temporale ha però dei costi sociali, che consistono soprattutto in una restrizione delle possibilità future di comportamento degli individui; il rischio al quale si sottopone il diritto è quello di rendere devianti, se non criminali, determinati individui o organizzazioni, senza conoscere in anticipo le intenzioni o le motivazioni dei loro eventuali comportamenti devianti.

Il diritto discrimina e decide per gli uni contro gli altri e lo fa per un futuro che non si può ancora prevedere.

I programmi che consentono al codice del diritto di diventare operativo sono costituiti dall'insieme delle norme e delle procedure. Questi programmi sono sempre condizionali e non di scopo. Le norme consentono di allocare i valori del codice ragione/torto a seconda dei casi che si presentano; in quanto programmi esse hanno la forma "se…allora…" e non sono stabilite in vista del raggiungimento di qualche scopo.

I programmi del sistema giuridico anticipano le condizioni che devono essere soddisfatte nel caso che subentri una certa situazione controversa e in questa loro apertura al futuro garantiscono al diritto una certa capacità cognitiva: la programmazione di tipo condizionale consente al sistema del diritto di distinguere chiaramente tra autoreferenza (concezione delle condizioni formali di rilevanza giuridica) ed eteroreferenza (argomentazioni sostanziali in caso di interessi lesi) e quindi anche tra ciò che è rilevante giuridicamente e ciò che non lo è. I programmi di scopo non consentono una discriminazione del genere poiché sono troppo legati ai casi specifici: una volta raggiunto lo scopo quale altra norma dovrebbe valere? Il diritto combina dunque formazione e cognizione in modo tale da garantire tanto la propria stabilità (le norme continuano a valere anche quando vengono deluse), quanto la propria capacità di apprendere (in caso di controversie di tipo nuovo si possono elaborare nuove normative).

Il diritto svolge una funzione di sistema immunitario per la società, poiché consente di reagire a delle situazioni impreviste senza una completa conoscenza dei fattori che hanno portato al disturbo (cioè alla contraddizione e al conflitto). Del resto, alle controversie giuridiche si giun-

ge di solito a partire da fattispecie non chiare e su questa produzione di controversie il diritto non ha nessun controllo: esso trasforma la sicurezza data dall'aspettarsi qualcosa come probabile nell'insicurezza prodotta dalla possibile delusione della norma.

3. Il diritto dei naviganti

Per descrivere, nella dimensione contemporanea, come il diritto stia elaborando il sovraccarico di aspettative che scaturiscono dalla diffusione delle tecnologie ICT, può essere utile stabilire un parallelismo di natura diacronica con quanto avvenne in passato in relazione al diritto dei naviganti per mare. Sarà possibile osservare come le similitudini non siano solo di carattere simbolico rispetto ai naviganti che solcano gli spazi della Rete.

La rivoluzione commerciale che ebbe inizio agli albori del secondo millennio fu stimolata dal rifiorire dei traffici marittimi, soprattutto nel bacino del Mediterraneo. Le cause di questo ridestato spirito commerciale, dopo un lungo periodo di ristagno, si possono rinvenire in una serie di fattori, tra i quali: l'organizzazione di un più efficiente sistema di comunicazioni per il trasferimento delle merci; l'introduzione di nuove e più sofisticate tecniche di scambio e di pagamento, che anticiparono, nella prassi, vari istituti del moderno diritto commerciale; l'intensificazione del volume dei traffici.

Il problema che si poneva, dal punto di vista giuridico, consisteva nella individuazione del diritto applicabile. Non esisteva, ovviamente, né un diritto internazionale come oggi lo conosciamo, né, tantomeno, un diritto della navigazione. Fu così che si consolidò un diritto di origine pattizia, sottratto alla regolamentazione statale, in cui erano gli stessi naviganti ad elaborare e codificare regole di tipo privatistico che disciplinavano i loro rapporti. Si trattava di una *lex mercatoria*[9], una norma a carattere consuetudinario, di origine prettamente sociale, nella formazione della quale era determinante l'influenza dei destinatari delle norme.

Con questo breve *excursus* si intende dimostrare che il diritto da molti secoli ha affinato espedienti normativi in grado di trattare questioni che i diritti nazionali non sono in grado di disciplinare.

[9] T. Treves, *Lex mercatoria dei naviganti*, in "Sociologia del diritto", nn. 2-3, 2005, p. 379.

Come nel Medioevo, oggi il diritto è chiamato a regolamentare un fenomeno che si caratterizza per la mancanza di frontiere fisiche, di collegamenti territoriali e – qui sta la novità più rilevante – di una dimensione spazio-temporale. Navigando in Internet, come è stato autorevolmente sostenuto[10], non si tocca alcun approdo spaziale, ma soltanto risultati visivi o uditivi: parole e suoni i quali risiedono nello spazio telematico che si distende sulla Terra come un sopramondo. Il navigante moderno non si sposta da un luogo fisico ad un altro ma si muove in un indefinito campo di energia rappresentato dal *cyberspazio*.

Anche l'esperienza maturata dai mercanti medievali, che solcavano gli oceani per commerciare i propri prodotti, fu, a suo modo, globalizzata; tuttavia, la peculiarità del fenomeno Internet sta non tanto nella "delocalizzazione", quanto nella sua "dematerializzazione", nella possibilità di trasferire contenuti digitali da un luogo all'altro del pianeta senza che nulla sia percepibile a livello sensoriale.

Il diritto, allora, deve decidere se e come intervenire: attraverso una fonte di carattere pattizio, ovvero con una fonte autoritativa; deve domandarsi se sia opportuno orientarsi verso un incremento dei meccanismi di controllo, ovvero in direzione dell'ampliamento degli spazi di libertà.

Posto che non pare ammissibile un situazione di anarchia per cui il c.d. villaggio globale dovrebbe riprodursi senza regole, occorre porre seriamente la questione della *governance* di Internet. Le ipotesi possono essere numerose: dal ricorso ad una regolamentazione internazionale o comunitaria, ad un modello fondato sul c.d. *soft law*, fino al ricorso alla *lex mercatoria*[11].

È proprio quest'ultima ipotesi che sembra maggiormente percorribile.

La riscoperta della *lex mercatoria*, inizialmente ad opera di giuristi francesi come Berthold Goldman e René David, è dovuta alla circostanza che l'affermazione della Rete globale prefigura la realizzazione di una società senza Stato, di dimensioni planetarie, retta da un diritto necessariamente sovranazionale, di formazione spontanea. Internet, che rappresenta il principale *medium* di comunicazione all'interno della società transnazionale, ha realizzato una vera e propria rivoluzione che non trova ispirazione

[10] N. IRTI, *Norme e luoghi. Problemi di geo-diritto*, Roma-Bari, Laterza, 2001, p. 65.

[11] C. ROSSELLO, *La governance di Internet tra diritto statuale, autodisciplina, soft law e lex mercatoria*, in "Diritto del commercio internazionale", n. 1, 2006, pp. 45 e ss.

in matrici filosofiche o politiche, in quanto essa si è autodeterminata e riprodotta solo a partire da se stessa.

Questa rivoluzione, che si è realizzata a livello sociale, ha prodotto, in ambito politico, una crisi della tradizionale dimensione statuale, con conseguenti ricadute nel sistema giuridico. Divenuti incerti i confini, erose le certezze del positivismo giuridico degli ultimi tre secoli, è apparso naturale gettare un ponte rivolto verso un passato in cui non si erano ancora determinate le condizioni per la nascita degli Stati moderni e si applicava quello che veniva chiamato *ius mercatorum*[12]. Si trattava di una legge senza frontiere, un sistema normativo sopranazionale ed autonomo, che consentiva agli operatori commerciali di disciplinare i propri rapporti di affari in modo assolutamente indipendente dai singoli diritti nazionali.

Il senso della moderna *lex mercatoria* è sfidare le pretese monopolistiche dello Stato legislatore. Le fonti di questo complesso normativo sono oggi considerate: i principî generali del diritto, il contratto, gli usi e la giurisprudenza arbitrale.

Nel dilemma tra l'adattare le vecchie regole alla nuova realtà e il creare nuove regole, anche attraverso il ricorso a nuovi modelli giuridici, il navigante del Duemila, ha certamente già optato per la seconda ipotesi.

4. Possibilità e limiti del diritto nell'età tecnologica

Alla luce di quanto esposto innanzi, alcuni presupposti della concezione illuministica dello Stato di diritto devono essere ripensati. Non è più consentito illudersi che il diritto possa soddisfare tutte le pretese e le istanze che l'incremento della complessità sociale gli pone sotto forma di aspettative. Appare obsoleta, altresì, l'immagine giusnaturalistica di una società costituita da individui liberi che delega allo Stato il potere di regolarla tramite il diritto. Piuttosto, occorre eliminare le ipersemplificazioni del senso comune e tentare di descrivere le possibilità e i limiti del moderno diritto nell'età tecnologica.

È ricorrente l'affermazione secondo cui nella società contemporanea sarebbe necessario un livello più elevato di legalità. Il problema sorge nel

[12] V. Ferrari, *Quesiti sociologici sulla lex mercatoria*, in "Sociologia del diritto", nn. 2-3, 2005, pp. 7 e ss.

momento in cui si debba interpretare il significato di "maggiore legalità". Nella vulgata del senso comune, fatta propria da larghi strati della politica, l'incremento della legalità si otterrebbe attraverso un sovraccarico di produzione normativa, secondo l'equazione: più diritto uguale più sicurezza delle aspettative. In senso diametralmente opposto, si sostiene che più regole comportano maggiore condizionamento dei cittadini, senza che a ciò corrisponda un incremento della sicurezza. Secondo questa tesi, la ipergiuridificazione, anziché risolverli, causerebbe un'amplificazione dei conflitti; la funzione del diritto, infatti, non è quella di eliminare i conflitti ma di trasformarli in contenziosi di natura giuridica e giudicarli secondo le proprie regole. L'equazione, in questa ipotesi, sarebbe: più diritto uguale più conflitti.

Muovendo da questi presupposti, una parte della dogmatica giuridica reinterpreta il bisogno di legalità come maggior possibilità di far valere pretese di diritto soggettivo, innanzitutto attraverso una autolimitazione dell'intervento dello Stato. In questa direzione, gli spazi che il diritto delle nuove tecnologie è riuscito a sottrarre alla regolamentazione degli ordinamenti statuali possono contribuire alla costruzione dei diritti di libertà[13] secondo principî e modalità assolutamente nuovi.

Libertà che non deve essere confusa con anarchia, con la negazione del diritto. Limitare l'intervento degli Stati nella regolamentazione di ambiti come la Rete globale non può significare, come pure è stato sostenuto[14], escludere la possibilità di applicare la categoria del giuridico, sollevare il ciberspazio dalla soggezione al principio di responsabilità.

Occorre, piuttosto, arricchire di nuovi contenuti la semantica di concetti classici della "teoria dello Stato" quali "sovranità" e "democrazia"[15]. Fermo restando il potere dei singoli Stati nazionali di esercitare il diritto di sovranità sui propri territori, si deve prendere atto che il riferimento a

[13] È il caso di ricordare come, storicamente, i primi diritti fondamentali si siano affermati come istituzioni che hanno il compito di difendere il cittadino nei confronti degli abusi dello Stato assolutista. Cfr. N. LUHMANN, *I diritti fondamentali come istituzione*, Bari, Laterza, 2002.

[14] J.P. BARLOW, *A Declaration of the Independence of Cyberspace*, in http://en.wikipedia.org/wiki/A_Declaration_of_the_Independence_of_Cyberspace.

[15] Cfr. A.C. AMATO MANGIAMELI, *Informatica, filosofia, diritto. Un'introduzione*, in "Filosofia e Diritto nell'era di Internet", Roma, Aracne, p. 27.

frontiere fisiche è privo di senso rispetto a Internet, che è strutturata sulla base di locazioni logiche e non geografiche. Di conseguenza, la forma stessa della sovranità e la sua capacità di esercizio devono essere rimodulate contemplando nuovi confini oltre a quello tradizionalmente riconosciuto del dominio riservato (*domestic jurisdiction*). Con riferimento al concetto di democrazia, la Rete può favorire un ampliamento degli spazi di esercizio di forme di partecipazione diretta dei cittadini alla gestione della cosa pubblica. L'idea di una democrazia digitale (*E-democracy*) non è più un'utopia e molti Paesi si stanno attrezzando per favorire, attraverso le nuove tecnologie, la partecipazione dei cittadini al processo democratico e facilitare l'esercizio dei diritti civili e politici sia in forma individuale che collettiva[16].

Il sistema giuridico non tollera lacune, insegnavano i giuspositivisti. Di fronte a questa massima e osservando le difficoltà degli ordinamenti nazionali a regolamentare il fenomeno della Rete, una parte della dogmatica è entrata in crisi, quasi che le fondamenta stesse del sistema giuridico stessero per cedere sotto la spinta delle schiere di neovolgari cibernauti.

In realtà, il problema rilevante non è se nell'ordinamento statale si rinvenga o meno una lacuna rispetto alla regolamentazione della Rete; piuttosto la questione fondamentale appare la seguente: è possibile che dalle problematiche sorte con riferimento alla regolamentazione di Internet, quale fenomeno sociale, siano scaturite soluzioni di natura tecnico-giuridica in qualche modo innovative rispetto alla tradizione?

In altri termini, occorre domandarsi se non stiamo assistendo ad un processo di adattamento del sistema giuridico alle istanze che provengono dall'ambiente e se il risultato di questo processo non rappresenti una acquisizione evolutiva, una condizione per trattare in maniera diversa casi differenti. L'attuale contingenza, letta in questo senso, può rappresentare un'opportunità, anziché un limite per il diritto.

Il sistema delle fonti, come si è cristallizzato nel corso dei secoli, fondato sulla statualità del diritto, sul primato della legge, sulla centralità costituzionale del principio di legalità, appare, per certi aspetti, inadeguato a misurarsi con le questioni legate alla globalizzazione e all'introduzio-

[16] Questi principî sono stati affermati nell'art. 9 del d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale).

ne delle nuove tecnologie. Come in ambito economico si realizza l'integrazione dei mercati, in ambito politico si compie la transizione verso la tecnodemocrazia, nel sistema giuridico la *lex mercatoria* si impone rispetto ai principî di statualità e nazionalità del diritto. Ciò che si prospetta, all'inizio del terzo millennio, è una società senza Stato, di dimensioni planetarie, retta da un diritto sovranazionale a formazione spontanea definito, appunto, *Nuova lex mercatoria*[17].

Si tratta di un diritto elaborato dal ceto imprenditoriale, senza la mediazione del potere legislativo degli Stati, formato da regole destinate a disciplinare in modo uniforme i rapporti commerciali che si instaurano entro l'unità economica dei mercati[18]. Questo diritto di origine privata si colloca al di fuori del sistema delle fonti, ma viene riconosciuto quale diritto valido ed efficace. La Corte di Cassazione, con sentenza n. 722 del 8 febbraio 1982, ne ha confermato il carattere di ordinamento giuridico originario, regolante il commercio internazionale.

Se il diritto degli ordinamenti nazionali è entrato in crisi, il sistema giuridico, nel suo processo evolutivo, sta tentando di elaborare nuove forme attraverso cui continuare a riprodursi. Il percorso che pare aver intrapreso è quello dell'affermazione di una legge senza frontiere che consenta di disciplinare i rapporti giuridici in modo indipendente sia dai singoli diritti nazionali che dal diritto internazionale pubblico. Un sistema normativo particolarmente adatto a regolare i rapporti tra privati, consumatori e aziende all'interno della Rete.

Diverso problema è quello della *governance* di Internet, una questione che pare difficilmente risolvibile con il ricorso a norme di carattere pattizio quali la *lex mercatoria*. Si tratta di un tema che merita ulteriori approfondimenti e rappresenta, per il diritto, un *casus irreducibilis* tuttora in attesa di soluzione.

[17] F. GALGANO, *Prefazione* al Trattato di diritto commerciale e di diritto pubblico dell'economia, vol. XXVII, Il contratto telematico, Padova, Cedam, 2002, p. 14.

[18] La definizione è di Galgano ed è tratta da *Diritto civile e commerciale*, I, Padova, Cedam, 1999, pp. 89 e ss.

Abstracts in inglese e italiano

Abstracts in inglese e italiano

LAURA ABBA, STEFANO TRUMPY

La *enhanced cooperation* per le politiche pubbliche di gestione delle risorse critiche di Internet

Enhanced Cooperation among Governments in Order to Manage the Internet Governance and the Critical Related Issues

The present report seeks to take stock of steps taken for *enhanced cooperation* on the management of Internet critical resources (domain names and IP numbers) to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet.

Even if the Internet governance is not restricted to the activities of governments, in recent years, heads of state and government acknowledged that the Internet system is a central element of the emerging information society, essential to provide a baseline level of services to every resident of a country [security, health, ...]. Internet is a global system; UN has been fully engaged in the Internet governance debate, since the need of international agreement and regulation became more apparent. However there are different positions about Internet coordination, operation, development, regulation, and legislation.

The World Summit on the Information Society (WSIS) reaffirms that governments have to achieve their full potential and to attain internationally agreements to build a people-centred, inclusive and development-oriented Information Society. Therefore, governments should take action, in the framework of national development policies, in order to support Internet governance and related issues, as well as to maintain the security, continuity and stability of the Internet, and to protect the Internet and other ICT networks from threats and vulnerabilities.

The international community is committed to harmonise present set of governmental positions and steps that are significantly not matching:

some governments prefer to participate directly in the Internet system management; others – like Italian Government – are working to increase governmental participation inside the existing international organisation, which are managing Internet, like ICANN.

* * * * *

Scopo di questo articolo è fornire un quadro di riferimento che possa contribuire a comprendere le questioni che muovono intorno al processo della *enhanced cooperation* sulla gestione delle risorse critiche di Internet (nomi a dominio e indirizzi IP) e ai ruoli e alle responsabilità dei Governi del mondo nella definizione, coordinamento e implementazione di politiche pubbliche per la Rete. Negli anni recenti i Capi di Governo hanno riconosciuto che Internet è un elemento centrale dell'emergente società dell'informazione, essenziale per il mantenimento delle funzioni vitali della società come la salute, la sicurezza e il benessere economico e sociale dei cittadini. Tuttavia, pur essendo universalmente riconosciuto che stiamo trattando un sistema globale – dove le questioni di politica pubblica richiedono accordi internazionali e non a caso sono argomento nell'agenda dell'ONU – esistono punti di vista diversi sull'adeguatezza dei meccanismi e delle attuali istituzioni globali che gestiscono i processi e sviluppano le politiche per Internet.

Dal Vertice WSIS 2003-2005, che l'ONU organizzò sulla costruzione della società dell'informazione, emerse con chiarezza il fatto che le politiche pubbliche per Internet sono una questione di ordine internazionale: a partire dalle svariate faccende legate allo sviluppo della stessa Società dell'Informazione sino al riconoscimento che tutti i Governi devono partecipare alla *Internet governance* su base paritetica per garantire la stabilità e la sicurezza del sistema e la continuità dei servizi. Nella comunita? internazionale esiste tuttavia una grande varieta? di pareri difficilmente armonizzabili: alcuni sono a favore di una partecipazione piu? diretta dei Governi nella gestione dell'Internet, per altri – come il Governo italiano – basterebbe invece accrescere la presenza dei Governi all'interno delle esistenti organizzazioni internazionali che gestiscono la Rete, come ICANN.

DAVIDE DE GRAZIA

L'Internet *Governance* tra tecnica, politica e diritto

The Internet Governance among Technology, Politics and Law

The Internet Governance, in the strict sense, can be defined as the whole functions and decisional processes which object is the management of physical and, above all, logical facilities which are the mean of Internet communication. This management requires a "collective action, by governments and/or the private sector operators of the networks connected by the Internet, to establish agreements about the standards, policies, rules, and enforcement and dispute resolution procedures to apply to global internetworking activities."

Since 1998, these functions are performed by Internet Corporation for Assigned Names and Numbers, a not-for-profit corporation located in Marina del Rey and subject to California Corporations Code rules.

The "rhetorical cloud" that so far has wrapped ICANN hid the real nature of the corporation functions to the public opinion. The myth of the purely technical nature of these functions is often used as an *escamotage* in order to elude the problem of political and democratic accountability of ICANN.

In performing its duties, ICANN takes measures, such as definition of namespace borders, new Top-level Domains creation, registry functions delegation, registrar accreditation, definition of policies related to numeric and alphanumeric identifiers and dispute resolution policies. Analysis of these decisions and acts convinces that we are not at the presence of pure technical coordination, but of typically political and administrative functions that affect fundamental rights and freedoms as freedom of speech, association, press, enterprise, and so on.

ICANN activity is strongly conditioned by U.S. Government, that keeps a "life-or-death power" over the corporation authority over the Internet root.

Times are now mature for the problem of global Internet Governance to be faced starting from the fundamental principle of rule of law.

* * * * *

L'*Internet Governance* "in senso stretto" può essere definita come l'insieme delle funzioni e dei processi decisionali che hanno ad oggetto la gestione

delle infrastrutture, fisiche ma soprattutto logiche, che costituiscono il veicolo della comunicazione via Internet. Tale gestione richiede una "azione congiunta, dei governi e/o degli operatori privati delle reti interconnesse, tendente a stabilire accordi relativi agli standards, alle *policies*, alle regole, alla loro applicazione e alle procedure di risoluzione delle controversie che devono trovare applicazione con riguardo alle attività di interconnessione globale".

Dal 1998 queste funzioni sono svolte dall'Internet Corporation for Assigned Names and Numbers, società senza fini di lucro con sede a Marina del Rey e soggetta alle disposizioni del California Corporations Code.

La "nuvola retorica" che fino ad oggi ha avvolto l'ICANN ha nascosto alla vista dell'opinione pubblica internazionale la vera natura delle funzioni esercitate dalla *corporation*. Il mito del carattere meramente tecnico di queste funzioni ha costituito il facile *escamotage* per eludere il problema della legittimazione politico-democratica dell'ICANN.

L'analisi degli atti e delle decisioni (dalla definizione dei confini del *namespace* alla creazione di nuovi nomi di dominio di primo livello, alla delegazione delle funzioni di *registry*, all'accreditamento dei *registrar*, alla definizione delle *policies* relative all'uso delle risorse numeriche e alfanumeriche di identificazione, alla risoluzione dei relativi conflitti) convince però che si è in presenza non di mero coordinamento tecnico, ma di esercizio di funzioni propriamente politico-amministrative, incidenti su diritti e libertà fondamentali come la libertà di manifestazione del pensiero, di associazione, di stampa, di iniziativa economica e così via.

L'attività dell'ICANN è fortemente condizionata dal governo statunitense, che mantiene tuttora un "potere di vita o di morte" sulla autorità della *corporation* sulla radice di Internet.

I tempi sono ormai maturi perché il problema della legittimazione globale allo svolgimento di queste funzioni sia finalmente affrontato a partire dal fondamentale principio della *rule of law*.

ANTONIO A. MARTINO

Libertà e regolazione in Internet. A proposito della *Governance*

Freedom and Rules in the Internet. About Internet Governance

The aim of this work is to show that you can present the Internet as a system and then pay attention to governance and government. Only within the rules you can implement freedom, and that this adjustment should be as universal as possible, given the nature of the set object (not to mention the social and political contexts which must be implemented) and contain as few rules as possible. Legislation must be laconic with words. At the same time it addressed the issue of government regulation of the Internet as urgent.

If the Internet is a system, necessarily it can be described as follows: composition (C), environment (E), structure (S) and mechanism (M) of the system.

- Adaptation, which is fixed by the ratio of the system with the external environment, within which is located and with which, in turn, interacts.

- The pursuit of objectives which is to mobilize the energies of the system towards the goals that were proposed.

- The integration, which is defined by actions that help to maintain the system consistency.

The composition of the Internet (C)

1. a global network of computer networks.

2. all resources on each computer and are accessible through the links between the networks.

The environment of the Internet: covers virtually all the Earth.

Internet space is an elsewhere. On the contrary, is one of many pieces of the complex puzzle in which we live: a complicated environment, inhabited by communities who live at different speeds.

The structure of the Internet (S) is a web of computers connected in a myriad of networks, the information is concentrated in terminals called hosts, with the protocol to have access to TCP / IP addresses.

Are also structure of the way of how the Internet is organized and governed by an institution that provides ICAAN to standards and other technical legal rules. ICANN, ISOC, and its related organizations includ-

ing the IETF (Internet Engineering Taskforce), which develops Internet standards, W3C that oversees the development of the WWW technology, intergovernmental entities such as the ITU (International Telecommunications Unit of the United Nations), WIPO (World Intellectual Property Rights)

- The mode is set up to practice where you actually practice Internet connections.

- Adaptation, which is fixed by the ratio of the system with the external environment, within which is located and with which, in its turn, interacts.

- The pursuit of objectives which is to mobilize the energies of the system towards the goals that were proposed.

The first objective of the Internet is always work and work anywhere.

- The integration, which is defined by actions that help maintain system consistency.

Treat the Internet as a system allows us to look at his element, environment, structure and mechanism. Few is being done on real government still lacks a strong international legal status of the Internet that recognizes its universality and thus face more difficult untimely interventions of national states that are against development, utility and freedom.

* * * * *

Lo scopo di questo lavoro è mostrare che si può presentare Internet come un sistema, interessandosi quindi tanto alla sua *governance* che al suo governo.

Con riguardo alla *governance* di Internet, si sosterrà che, poiché solo all'interno di un complesso condiviso di regole si può attuare la libertà in/di Internet, la sua regolazione dovrebbe essere la più universale possibile data la natura dell'oggetto regolato (senza dimenticare i contesti sociali e politici in cui tali regole verranno attuate) e la più sobria possibile, nel rispetto del principio per cui è bene che la legislazione sia avara di parole.

Con riguardo al governo di Internet, si sottolineerà innanzitutto l'urgenza di affrontare il tema della regolazione del governo della Rete. A tal fine, Internet verrà concepito come un sistema che presenta le seguenti caratteristiche:

- la descrizione della composizione (C), dell'ambiente (E), della struttura (S) e del meccanismo (M) del sistema;

- l'adattamento, che è determinato dal rapporto del sistema con l'ambiente esterno, all'interno del quale si trova e con il quale, a sua volta, interagisce;
- il perseguimento degli obiettivi cui il sistema è preposto, mediante la mobilitazione delle energie necessarie;
- l'integrazione, che è definita dalle azioni che aiutano a mantenere la coerenza del sistema.

Trattare Internet come un sistema ci consentirà di esaminare i suoi elementi peculiari, e cioè l'ambiente, la struttura e il meccanismo, oltre che di studiare le sue procedure interne e di verificare che anche sotto il profilo giuridico-politico Internet di presenta come un insieme degno di speciale attenzione, perché mai studiato sistemicamente. Ed è un peccato, perché dall'ottica del sistema è più facile rilevare quali siano le caratteristiche e le pratiche che favoriscono la sua coesione ed il suo sviluppo e quali, al contrario, ne minacciano la sopravvivenza. Meglio ancora, per un'analisi giuridico-politica considerare Internet come sistema ci consentirà di discutere concretamente su quale parte dei componenti o del rapporto con l'ambiente o della propria struttura e soprattutto il meccanismo si possa migliorare.

Tutto ciò per mettere in evidenza come poco si sta facendo in materia di governo di Internet, mancando ancora a livello internazionale uno *status* giuridico definito. Uno *status* che riconosca la sua universalità e quindi renda più difficili gli interventi intempestivi degli Stati nazionali contrari allo sviluppo, all'utilità e, in una parola, alla libertà di/in Internet.

ALESSANDRO NICOTRA

L'Internet *Governance* in Italia

Internet Governance in Italy

Internet Governance isn't easy to translate in italian and to define exactly. The terms "gestione di Internet" (Internet management) or "governo della rete" (government of the network) used to translate "Internet Governance" in Italian, are formally correct, but they appear to be misleading and restrictive if we refer both to the technical and public policy management.

Moreover, it'll be interesting to trace the short history of the network in order to understand why we moved from a narrow meaning of "Internet governance" (understood as the technical management of the Net, ie pertaining to the management of DNS root server infrastructure and technical standards) to a broad meaning which covers a range of other related issues such as: net neutrality, user's Internet access rights and costs, respect for fundamental freedoms, protection of intellectual property, security, that includes identifiying cyber crime and strategies to curb it.

The process to discuss public policy issues related to key elements of Internet governance was launched internationally inside the UN Summit on the Information Society - Geneva 2003 and Tunis 2005- and now it continues its march in the Internet Governance Forum. The Internet network development story shows that explains how Italy

has been among the first countries in the world to establish an Internet Governance Forum in order to facilitate the exchange of information and best practices at national level. In this regard CNR and ISOC Italy made a big efforts to fully make advantage of the expertise of the academic, scientific and technical communities.

Without defining the Internet Governance and starting this innovative multi-stakeholder IGF process to improve shared rules, the Internet could not continue to work and to evolve.

* * * * *

Definire o circoscrivere cosa si debba intendere per "Internet Governance" non è cosa semplice. Le espressioni "gestione di Internet" o "governo della Rete", usate per tradurre "Internet Governance" in ital-

iano, sono formalmente corrette, ma nella sostanza risultano essere fuorvianti e limitative se riferite indistintamente tanto alla gestione tecnica quanto alla gestione "politica" di Internet.

Risulta utile, quindi, ripercorrere la giovane storia della Rete per comprendere il perché si sia passati da un significato stretto dell'"Internet Governance", intesa come gestione tecnica di Internet (afferente cioè alla gestione del DNS, dei Root Server, delle infrastrutture e degli standard tecnici), ad un'accezione più estesa nella quale rientrano tutta una serie di altri aspetti correlati, quali ad esempio: la neutralità della Rete, il diritto ed i costi di accesso, il rispetto delle libertà fondamentali, la tutela della proprietà intellettuale, la sicurezza, l'individuazione di ciò che è reato e la correlata punibilità o repressione e via discorrendo.

Il processo costituente per una Internet Governance in senso esteso è stato avviato a livello internazionale dall'ONU con l'organizzazione dei due summit sulla Società dell'Informazione di Ginevra nel 2003 e di Tunisi nel 2005 e prosegue con l'Internet Governance Forum. Lo storia dello sviluppo della Rete in Italia illustra il percorso che ha portato il nostro ad essere fra i primi paesi a raccogliere l'appello e l'opportunità di costituire un Internet Governance Forum nazionale, attraverso un confronto ed un coinvolgimento bipartisan, avvenuto grazie in particolar modo alle sollecitazioni ed agli sforzi compiuti in particolar modo dal CNR e da ISOC Italia.

Nel definire il "governo di Internet" l'unico dato certo è che senza partecipazione e senza regole condivise tra gli stakeholder, Internet non funziona e si spegne.

RITA ROSSI

La qualificazione giuridica del nome a dominio

The Juridical Notion of the Internet domain name

The issues regarding the juridical nature of a domain name have developed enormously with the worldwide expansion of the commercial use of the Internet. On the one hand, it is a technical resource essential for access to the Internet, and on the other hand, it is a distinguishing mark of commercial activity which potentially can enter into conflict with the pre-existing rights of other subjects. Also in Italy, due to the significant domain hoarding phenomena which have already occurred in the more technologically advanced nations, jurisdiction has often had to deal with this question, recognising the potential of a domain name to damage pre-existing rights and deciding, for the most part, in favour of the possessor of those rights with respect to the owners of Internet domains.

The Italian Law on Industrial Property (Legislative decree n°. 30/2005) regulates company domain names, including them within the unified principle of distinguishing signs. This is a relevant ruling which, however, does not avoid the doubts that the interpreter might have regarding the nature of the new sign, because the legislation regards only company domain names. Before the Law on Industrial Property, in Italy there existed only the set of provisions contained in the Law of Electronic Communications (Legislative decree n°. 259/2003). This law accepted the EU directives in the sector of electronic communications. At article 15, entitled "Numbering, assignment of domain names and guidance it established supervision on the part of the Ministry of Economic Development.

The Italian authorities put in charge of the assignment and management of first level domain names (general top level domain (gTLD) and country code top level domains, ccTLD), operate under delegation issued by the Internet Corporation for Assigned Names and Numbers (ICANN), the United States authority responsible, among others, for the assignment of codes to the gTLD and ccTLD. These authorities have regulations for the management of this specific sector. These are essentially agreed rules and not specific national legislation of positive law. In conformity with the above mentioned rules today there are millions of

domain names registered and this enables individual users, institutions and companies to know, work and produce with the Internet.

The domain name constitutes a new asset of a dual nature. It is both a technical resource and a juridical property, open to economic assessment, an object of acts of conveyance, an asset assuming differing values according to the various contexts in which it functions. It is an opportunity, and at the same time a challenge, for the jurist who must deal with the new problems deriving from the advent of the Internet. The Web is not only where technology has modified the ways of verifying a fact, but where it increasingly reflects on the whole system of reference, thwarting the traditional concept of territorial borders.

* * * * *

La problematica intorno alla natura del nome a dominio visto, da un lato, come risorsa tecnica indispensabile a consentire il collegamento e la presenza in Internet, e, dall'altro, quale segno distintivo dell'attività commerciale potenzialmente idoneo ad entrare in conflitto con preesistenti diritti di altri soggetti, si è enormemente sviluppata con l'espandersi dell'Internet commerciale in tutti i Paesi. Anche in Italia, a causa di consistenti fenomeni accaparratori già verificatisi in altre nazioni a più avanzata vocazione tecnologica, la giurisprudenza si è occupata sovente della questione, riconoscendo al nome a dominio la sua attitudine a ledere preesistenti diritti e decidendo, a grande prevalenza, in favore dei possessori di quei diritti rispetto ai titolari dei domini.

Il Codice sulla proprietà industriale (decreto legislativo n. 30/2005) ha disciplinato i nomi a dominio aziendali riportandoli sotto il principio di unitarietà dei segni distintivi. Si tratta di una disposizione rilevante che tuttavia non fuga i dubbi che l'interprete continua a porsi intorno alla natura del nuovo segno, poiché la disciplina in discorso ha riguardato soltanto il nome a dominio aziendale. Prima del citato Codice della proprietà industriale nel nostro Paese esisteva solo la normativa contenuta nel Codice delle comunicazioni elettroniche (decreto legislativo n. 259/2003), di recepimento delle direttive comunitarie nel settore delle comunicazioni elettroniche, il quale disciplinava all'articolo 15 (rubricato "Numerazione, assegnazione dei nomi a dominio e indirizzamento") la vigilanza del Ministero dello sviluppo economico.

A ciò si aggiunga, però, che le autorità preposte alla assegnazione e gestione dei nomi a dominio di primo livello (*general top level domain* - gTLD e *country code top level domain* -ccTLD), operanti in virtù di opportuna delega rilasciata dall'*Internet Corporation for Assigned Names and Numbers* (ICANN), l'autorità statunitense responsabile, fra gli altri, dell'assegnazione dei codici ai gTLD e ai ccTLD, dispongono di specifici regolamenti per la gestione del settore. Si tratta per la maggioranza di normative concordate e non di specifiche norme nazionali di diritto positivo. In conformità alle predette discipline sono oggi registrati milioni di nomi a dominio e ciò permette agli individui, alle istituzioni, alle imprese di conoscere, lavorare, e produrre con la rete Internet.

Il nome a dominio costituisce dunque, un nuovo bene di natura duale: risorsa tecnica, da un lato, e bene giuridico, dall'altro. Si tratta in ogni caso di un bene suscettibile di valutazione economica, potendo essere oggetto di atti di alienazione, e che presenta nei vari ambiti in cui viene a esistenza caratteri molto diversi tra loro.

L'interesse del giurista per tale tema è quindi molto forte, costituendo esso un'occasione e una sfida allo stesso tempo proprio per quel giurista che intenda misurarsi con i problemi nuovi derivanti dall'avvento dell'Internet, una tecnologia che ha modificato non solo i modi del verificarsi di un fatto, ma ha finito per riflettersi sull'intero sistema giuridico di riferimento, a partire proprio dalla vanificazione del tradizionale concetto di territorio.

DANIELA MESSINA

Le prospettive del diritto all'oblio nella Società dell'informazione e della comunicazione

The Perspectives of the Right to Oblivion in the Information and Communication Society

The aim of this study is to analyze the relevance of the right to forget and the different ways to safeguard the subjective legal status within the Internet era, which have had a deep influence on the traditional people's self perception as both human being and member of society.

Allowing for a disruption of space-temporal borders and a reinforcement of the information storage, indeed, new technologies have taken the role of essential tools in order to the data storage, changing the perception of collective memory.

There is no doubt that information activities, above all, have undergone considerable changes in the last years. In particular, nowadays news remain imprisoned within a virtual net preventing people from forgetting. In this context, the right to forget comes to light as a new demand of private sphere protection, based on the persons' right to preclude anyone from distorting theirs identity because of an unjustified reiteration of old news. That's because there is no reason to believe that present identities have to correspond to the past ones.

However, it's necessary to establish a right balance between the right to forget and the right to information, trying to find the equilibrium point between the right to tell about daily goings and the fundamental right to preserve the natural development of the personal identity against the risk of not update news spreading.

This goal has been achieved through the doctrine and the jurisprudence's work because of the absence of a legislative intervention addressed to recognize the right to forget. Later, the Privacy Protection Law allowed to improve the interpretation activity, but the advent of information technology has introduced many other hurdles to overcome. A proposed law currently pending in the Italy legislature, but at the same time useful in-depth elements comes from a comparative analysis, with particular regard to France's experience. Both tests

shoots for the recognition of the right to forget as a right deserving a constitutional protection, separated from that dedicated to privacy and personal identity right.

* * * * *

Il lavoro si propone di analizzare la rilevanza del diritto all'oblio e le possibili forme di tutela di tale situazione giuridica soggettiva in un'era, quella della Rete, che sta progressivamente cambiando la percezione che l'uomo ha di sé come individuo e come membro di una comunità. Favorendo l'abolizione dei confini spazio-temporali ed il potenziamento della capacità di memorizzazione, le nuove tecnologie si stanno infatti imponendo come indispensabile strumento di archiviazione dei dati, arrivando a modificare la stessa percezione collettiva del passato. Le conseguenze di tale cambiamento risultano evidenti in particolar modo nell'ambito dell'attività di informazione dove oggi si pone il problema dell'impossibilità di "dimenticare", di consentire ancora che il tempo, come sempre, faccia il suo corso cancellando il ricordo relativo ad un avvenimento, un protagonista (talvolta involontario) o una vicenda, dal momento che la notizia risulta molto spesso imprigionata in una rete non più fisica, ma virtuale. Da qui l'accentuarsi dell'esigenza collettiva di una rilettura e valorizzazione del diritto all'oblio come esigenza di tutela della propria sfera privata, basata sul diritto a non veder distorta la propria immagine attuale a causa di un'ingiustificata reiterazione di notizie relative a vicende o affermazioni che in passato lo hanno visto protagonista, ma che non corrispondono più a quella che è l'attuale proiezione dell'identità di un individuo all'interno della società. Occorre tuttavia bilanciare la tutela del diritto all'oblio con la libertà di informazione, ricercando un punto di equilibrio tra il diritto di narrare gli avvenimenti e di informare i consociati ed il fondamentale diritto del singolo a non veder minata la naturale evoluzione della propria personalità con una nuova diffusione di notizie che ripropongono un'identità cristallizzata, mai evolutasi nel tempo e, quindi, spesso non corrispondente all'attuale ruolo dell'individuo nella società.

Il lavoro di bilanciamento è stato svolto in passato essenzialmente dalla dottrina e dalla giurisprudenza, in assenza di un intervento legislativo volto a riconoscere il diritto all'oblio come diritto soggettivo costituzio-

nalmente garantito. Successivamente, l'introduzione della normativa sul diritto alla tutela dei propri dati personali ha consentito di porre alcuni punti fermi nell'attività di interpretazione, ma restano oggi ancora alcuni nodi insoluti legati proprio all'avvento delle nuove tecnologie e all'uso crescente di queste ultime a scopo informativo. Un disegno di legge è attualmente in discussione in Parlamento, ma elementi di utile approfondimento vengono anche dall'esperienza comparata, con particolare riferimento ad un progetto di legge francese. In entrambi i testi in discussione, nei quali non mancano luci ed ombre, appare presente la volontà di riconoscere il diritto all'oblio quale diritto meritevole di tutela autonoma e distinta dai pur fondamentali diritti alla riservatezza e all'identità personale, nel pieno rispetto dei rispettivi dettati costituzionali. Se, infatti, obiettivo comune delle carte costituzionali è quello di garantire i diritti inviolabili ed indispensabili per un adeguato e corretto sviluppo della personalità di un individuo nella società anche e soprattutto in linea con l'evoluzione che inevitabilmente la contraddistingue, il diritto all'oblio si pone come ulteriore strumento di tale adempimento, legittimato dalle nuove esigenze che proprio quel progresso inarrestabile ha portato alla luce.

JEANNE PIA MIFSUD BONNICI

Protecting Informational Privacy in Cyberspace Exploring Complementary Routes

La protezione dei dati personali in Internet Alla ricerca di metodi di tutela complementari

Nel mondo di Internet, se da un lato risulta estremamente facile raccogliere ed utilizzare informazioni di carattere personale, dall'altro non esistono adeguate forme di tutela della riservatezza di quelle stesse informazioni laddove esse vengano impiegate per scopi commerciali. Fino ad oggi l'orientamento degli Stati nazionali è stato quello di adottare legislazioni mirate alla protezione dei dati personali, aventi ad oggetto la salvaguardia del diritto fondamentale alla *privacy,* e al contempo di favorire l'adozione da parte delle imprese commerciali di linee guida e prassi volte alla tutela della privacy del consumatore/utente. Si tratta però di interventi insufficienti, che spesso non sono in grado di proteggere adeguatamente i consumatori dall'utilizzo abusivo dei loro dati personali.

Nel presente lavoro l'autrice conduce una riflessione sul ruolo svolto dalle legislazioni in materia di protezione dei dati personali, con particolare riguardo ai profili della tutela delle informazioni personali in Internet. Più in particolare, l'autrice prende in esame due distinte ipotesi: il caso di dati personali persi con negligenza o rubati; e il caso di dati personali in possesso di imprese commerciali che, consociandosi, mettono insieme i propri patrimoni informativi. Con riguardo ad entrambe queste due ipotesi l'autrice propone metodi di salvaguardia dei dati personali nuovi e/o integrativi rispetto a quelli già previsti dalle legislazioni vigenti in materia. Il primo si basa sulle teorie correnti di diritto pubblico internazionale, nelle quali si profila una responsabilità del settore privato in materia di diritti fondamentali. Il secondo metodo, invece, prevede il ricorso alle politiche sulla concorrenza per attivare sistemi di protezione dei dati personali. In conclusione, l'autrice evidenzia i benefici che i consumatori possono trarre dall'utilizzo dei due nuovi metodi di tutela della *privacy* appena ricordati, pur in presenza di incertezze e dubbi circa la loro applicazione.

* * * * *

On the Internet it extraordinarily easy to collect and use personal information, while there are few incentives in favour of the respect of privacy over use of personal information for commercial purposes. To date, states have sought to protect the fundamental right of privacy by specific personal data protection legislation and by encouraging businesses to adopt privacy policies and practices to protect consumer/user privacy. These approaches have limited effects, leaving consumers often without any protection or remedies against abusive use of their personal information. This paper reflects on the role that data protection legislation have in the protection of informational privacy online. It looks at two specific scenarios: possible remedies where personal information has been negligently lost or stolen; and possible safeguards or remedies available when two or more private information-rich businesses merge or are taken-over online. In each scenario, an approach that can potentially complement the current systems of protection of personal information is presented. The first approach is based on current theories of public international law arguing for private sector fundamental rights responsibility and the shifting of liability of private sector liability to states in cases of breaches of fundamental rights. The second approach is a market-based approach using competition policy mechanisms to protect informational privacy. The paper argues in conclusion that in spite the uncertainties of these complementary approaches for the protection of informational privacy, consumers can benefit from their addition to protections offered by data protection legislation.

UGO PAGALLO

Privacy e Design

(Privacy by Design)

The paper examines today's debate on "privacy by design" and the idea that data protection should be embedded in ICT through default settings. On one hand, it seems possible to achieve the perfect enforcement of the law via design in order to solve, say, matters of jurisdiction on the internet. On the other hand, scholars often stress the technical unfeasibility of automatizing all the mechanism of data protection and highlight why self-enforcement technologies would erode the public understanding of the law by eliminating useful interfaces between the terms and the application of the law. In the light of the current state-of-the-art, the paper suggests that we should understand both people's privacy claims and data protection 'by' design, not 'as' design, that is, as if the goal were to design regulatory standards that hit their target with infallible accuracy. Both for technical and ethical reasons, it is unlikely that the science of design will offer the one-size-fits-all solution to the problems of data protection. Rather, as moral enablers, these technological devices offer the key to grasp how we are coping with today's privacy issues. An example is current work on AI & Law and legal ontologies which further illustrates how artificial intelligence and operation research may aid design and, in doing so, impact on the structure and evolution of legal systems. The stake is the integration of compliance with regulatory frameworks through data protection policies, so that privacy protection must ideally become a default mode of operation for ICTs.

* * * * *

Il saggio esamina l'odierno dibattito sulla "privacy by design" e l'idea che le misure a tutela dei dati personali debbano essere presenti, quali opzioni base, sin dalla fase di progettazione degli strumenti preposti al trattamento dei dati. Da un lato, mediante il design, sembra possibile garantire la perfetta applicazione della legge, sciogliendo, ad esempio, alcuni dei nodi di ripartizione delle competenze giurisdizionali in rete. D'altro canto, gli studiosi sottolineano sia le difficoltà pratiche cui si va incontro nel progettare sistemi esperti nel settore della privacy, sia il

rischio che l'automatizzazione del diritto stravolga la pubblica comprensione della legge, là dove eliminerebbe ogni mediazione tra il dettame normativo e la sua specifica attuazione. Alla luce dell'odierno stato dell'arte, la tesi del presente saggio è che la tutela dei dati personali vada intesa *attraverso* il design, non *come* design, e cioè come se lo scopo fosse quello di garantire, in modo infallibile, le finalità operative della legge grazie ad un insieme di accorgimenti tecnologici. Tanto per ragioni pratiche quanto per motivi etici, sembra infatti arduo pensare che la scienza del design possa mai offrire la chiave di volta per risolvere l'intero plesso dei problemi che affliggono l'odierna protezione dei dati personali. Piuttosto, attraverso gli accorgimenti tecnologici del design, si offre un punto di vista privilegiato per riflettere sul modo in cui affronteremo gli odierni nodi della privacy. Un esempio concreto è dato dalle ricerche sull'intelligenza artificiale e le ontologie giuridiche applicate ai temi della tutela e trattamento dei dati personali. La posta in gioco è data dall'irrobustimento dell'odierno quadro normativo mediante politiche del design, affinché il diritto alla privacy diventi idealmente opzione base nell'uso delle tecnologie dell'informazione e della comunicazione.

GIUSEPPE VACIAGO

Privacy e tutela dell'ordine pubblico in Europa e negli Stati Uniti: un differente approccio per raggiungere un difficile compromesso

Privacy, Public Order and Security in Europe and the US A Different Approach for a Difficult Compromise

Over the coming years a crucial issue in dealing with cybercrime will be the delicate balance that must necessarily be struck between personal data protection and public order and security.

If the stellar growth in e-commerce in the last decade, was accompanied by increasing alarm about the attendant potential for fraud (from e-bay scams to credit-card cloning), the next ten years seem bound to be beset by the headaches of cloud computing: who knows what dormant dangers may be inadvertently aroused merely by surfing the web, even without posting personal data online, or using social networks (all of which are exposed to data mining)?

In this specific context, given the enormous wealth and value of the information that can be gleaned from the hard drives of individual PCs or even a mere web search not to mention electronic intercepts, digital forensics and cloud computing are certain to play an ever more decisive role in criminal investigations.

In addition to the myriad issues which are bound to arise as cloud computing gathers momentum, law-enforcement agencies will be increasingly faced with conflicts of jurisdiction which rarely, if ever, arise in connection with house searches and wiretaps, but somehow seem to spontaneously emerge, almost out of thin air, whenever digital content is targeted.

Apart from the procedural complications (such as letters rogatory, and interpretations of international treaties and conventions) they entail, potential conflicts of jurisdiction also tend, more crucially, to lend decisive weight to legal, political, cultural and social differences in the ways that transnational issues, such as privacy, are dealt with in the various countries involved.

This article highlights commonalities and differences in the ways personal data protection has been approached in the U.S. and Europe (especially Italy), respectively.

* * * * *

Un tema di assoluta rilevanza, per il diritto dell'informatica, è il compromesso, difficile ma non eludibile, che si dovrà trovare tra tutela dei dati personali e tutela dell'ordine pubblico.

Se l'ultimo decennio è stato quello del commercio elettronico e delle conseguenti preoccupazioni legate alle possibili frodi (dalle truffe su e-bay alla clonazione delle carte di credito), il prossimo si preannuncia come quello del *cloud computing* e dei rischi collegati alla diffusione dei propri dati personali in Rete e specialmente all'interno dei *social network* (potenzialmente esposti al rischio di *data mining*).

In questo contesto l'investigazione digitale ha, ora più che mai, un ruolo determinante, in quanto il valore delle informazioni che la polizia giudiziaria può rinvenire, all'interno di un *personal computer* o attraverso un'intercettazione telematica o anche solo attraverso una semplice navigazione su Internet, è enorme.

Tuttavia, mentre nella perquisizione di un appartamento o in una intercettazione telefonica i limiti della giurisdizione nazionale non vengono quasi mai toccati, nel momento stesso in cui oggetto dell'indagine è il dato digitale quasi automaticamente insorge il conflitto tra diverse giurisdizioni, senza neppure arrivare a toccare i possibili problemi che saranno generati dalla sempre maggiore espansione del *cloud computing*.

Nel momento stesso in cui si crea un potenziale conflitto giurisdizionale non è solo rilevante l'aspetto procedurale (rogatorie, convenzioni e accordi internazionali), ma diventano determinanti le differenze giuridiche, politiche, culturali e sociali tra i vari Paesi, in una tematica trasversale come è sicuramente quella della protezione dei dati personali.

Obiettivo del mio lavoro è quello di offrire un'analisi comparativa del differente approccio tra Europa (con particolare riferimento all'Italia) e Stati Uniti su questo tema.

FRANCESCA BADOCCO

Riflessioni sul diritto d'accesso a Internet nell'ambito del diritto dell'Unione europea

The Right to Internet Access under the European Union Law

This paper aims to offer an answer to the question, which arises with the coming into force of the "telecom package" on 18 December 2009; that is the opportunity to acknowledge autonomy to the right to Internet access.

To do so, this investigation analyses the role played by the European Commission, looking at its relevant actions within this area and examines other institutions behaviour, notably that of the European Parliament.

The paper then turns to the analysis of the current telecommunications legal framework, dissecting the development of the "telecom package", highlighting the non-linear path it took during its formative stages. It emphasises the innovative interventions within the European Parliament as it evolved, as well as the European Commission positions on the right to Internet access aimed at encouraging the adoption of relevant measures which facilitate the exercise of that right.

The systematic reconstruction of the new regulatory framework, which comprises Regulation (CE) 1211/2009 establishing the Body of European Regulators for Electronic Communications (BEREC), the Directive 2009/136/CE, also known as "Citizens' Rights" Directive, and the Directive 2009/140/CE, also called the "Better Regulation" Directive, is considered. In particular, the provisions concerning the right to Internet access are analysed along with the principles arising from the relevant recitals.

As a consequence of the cross analysis of the resulting data it is possible to propose some positive conclusions about the autonomy of the right to Internet access. In particular, it would be correct to acknowledge a more extended autonomy of the relevant right at the European level compared to the international level, on the grounds of the independence of that right from the prejudice of any fundamental right connected to it.

* * * * *

Il contributo, prendendo le mosse dall'evoluzione della società dell'informazione nell'ambito dell'Unione europea, tenta di offrire una risposta

al quesito di stretta attualità, a seguito dell'entrata in vigore del "pacchetto telecom" il 18 dicembre 2009, se sia possibile riconoscere al diritto d'accesso ad Internet autonomia rispetto ai diritti fondamentali di cui permette l'espressione.

L'indagine si snoda attraverso l'esame del ruolo svolto dalla Commissione europea, con una panoramica sulle azioni dalla medesima promosse, e la valutazione in chiave positiva dell'atteggiarsi delle altre istituzioni, in particolare del Parlamento europeo, per approdare all'analisi dell'attuale quadro giuridico di riferimento in materia di telecomunicazioni.

Al riguardo, viene ricostruito il percorso, non sempre scandito da linearità, che ha condotto alla elaborazione del "pacchetto telecom". In particolare, si dà atto degli interventi di carattere innovativo emersi in sede parlamentare, nonché delle posizioni espresse dalla Commissione europea in materia di accesso ad Internet, per incoraggiare l'approvazione di misure in grado di permettere il concreto esercizio dello stesso.

Un particolare approfondimento è dedicato alla ricostruzione sistematica dei singoli provvedimenti (in particolare, il regolamento (CE) 1211/2009, istitutivo del nuovo organismo dei regolatori delle telecomunicazioni – BEREC –; la direttiva 2009/136/CE, nota come direttiva "diritti dei cittadini", e la direttiva 2009/140/CE, conosciuta come direttiva "migliore regolamentazione") che disciplinano la materia, concentrando l'attenzione sulle disposizioni che incidono, in modo anche indiretto, sul diritto d'accesso ad Internet, tenuto conto anche delle dichiarazioni contenute nei rispettivi considerando.

All'esito dell'analisi "incrociata" dei dati emersi, si giunge all'elaborazione di conclusioni favorevoli al riconoscimento dell'autonomia del diritto d'accesso ad Internet di portata, se possibile, più ampia rispetto a quella già riconosciuta a livello internazionale, prospettando l'indipendenza del medesimo dall'eventuale pregiudizio di uno dei diritti fondamentali dei quali permette l'estrinsecazione.

ELENA BASSOLI

La disciplina giuridica della seconda vita in internet L'esperienza *second life*

The Legal Framework of Second Life Experience on the Internet The Experience of "Second Life"

As is well known, the Internet is by its nature, without a defined territory and without a clearly defined space and time.

In fact, isn't the same machines that make it up, but it's synchronously everywhere and nowhere, so as to constitute a parallel world to the real world.

In a forthcoming developments is not difficult to predict even a psychological transformation of network users, as already happens in Second Life.

The Web discussions on Second Life began in 2003, when that three-dimensional virtual world was created by the Californian company Linden Labs.

Technically should speak of Massive Multiplayer Online Role-Playing Game (MMORPG), but its spread it is now a global social phenomenon.

To set a second life on the web is not a new idea. It has concerned and passionate writers of every kind and even movies have often made use of this artifice to tell the paradoxes of virtual lives, that are so different from real ones, but so intensely lived, that we can not distinguish reality from fiction, often leaving the reader in doubt that we lived every day is not the true reality.

Today, the time appears ripe to get to imagine a world increasingly interconnected and interoperable, where the virtual is more real than the reality.

Second Life is online game with different settings and without specific missions; the novelty of the game is the complete deconstruction, allows anyone to do almost anything. So Second Life, because of its connotation generalist and non-specific, like real life, well suited to represent a formidable legal training for the future, when our lives will probably increasingly virtualized and legal issues to be addressed will be new and unpredictable.

* * * * *

Internet è, come noto, per sua natura, delocalizzato, a-territoriale e privo di uno spazio e un tempo ben definiti. Esso, infatti, non si identifi-

ca con le macchine che lo compongono, ma è sincronicamente ovunque e in nessun luogo, così da costituire un mondo parallelo al mondo reale. In una evoluzione ormai prossima non è difficile prevedere una trasformazione anche psicologica degli utenti della Rete, che si muoveranno all'interno di essa per mezzo di propri *Avatar*, dotati di sembianze umane, ma privi di corporeità, come già accade in *Second Life*.

Del fenomeno *Second Life* in Internet si cominciò a discutere nel 2003, allorquando questo mondo virtuale tridimensionale venne creato dalla società californiana *Linden Labs*. Tecnicamente dovrebbe parlarsi di *Massive Multiplayer Online Role-Playing Game* (MMORPG), ma la sua diffusione ne fa ormai un fenomeno sociale a livello planetario.

L'idea di ambientare una seconda vita sulla Rete delle reti non è nuova. Essa ha interessato e appassionato scrittori di ogni genere e anche la filmografia ha spesso fatto ricorso a tale espediente per raccontare i paradossi delle vite virtuali, così dissimili da quelle reali, ma così intensamente vissute da non riuscire a discernere più la realtà dalla finzione, lasciando spesso al lettore il dubbio che quella vissuta da noi ogni giorno non sia la vera realtà.

Ad oggi i tempi appaiono maturi per arrivare a immaginare un mondo sempre più interconnesso e interoperabile, ove il virtuale è più reale del reale.

Second Life è un gioco *on line* con la diversità di non avere ambientazioni e missioni specifiche; la novità del gioco è la completa destrutturazione, consente a chiunque di fare pressoché qualsiasi cosa.

Così SL, proprio per la sua connotazione generalista e aspecifica, al pari della vita reale, ben si presta a rappresentare una formidabile palestra giuridica per il futuro, quando le nostre vite saranno, presumibilmente, sempre più virtualizzate e le questioni giuridiche da affrontare saranno nuove e imprevedibili.

MARIA CONCETTA DE VIVO

Viaggio nei metaversi alla ricerca del diritto perduto

Exploring Metaverses (Fictional Virtual Worlds) to Research the Lost Law

This article analyzes the phenomenon of virtual communities and legal issues arising. Many virtual companies, such as Second Life, considered as a game , is actually a real aggregations of individuals using the platforms to create different kinds of personal relationships even with economic interest.

The metaverses appears as virtual worlds where people live through a digital simulacrum to interact with others. The legal aspect of the personal identity is analyzed.

The example of Second Life allows us to study: the avatar, the different activities that a person can do in the metaverse, the relationship between law and metaverses, areas and fields of law, guarantees). This article exposes some interesting legal studies.

This brief study shows how these environments are seemingly distant from the reality of everyday life, but they are however useful tools for education (schools and universities, highlighting the best known e-learning) and new forms of electronic commerce. In both cases the right, until now virtually absent in these environments, is necessary and important.

* * * * *

Nel saggio viene analizzato il fenomeno delle comunità virtuali con le problematiche giuridiche connesse. Molte società virtuali come *Second Life* possono considerarsi non solo ambienti ludici bensì vere e proprie aggregazioni di individui che utilizzano le piattaforme informatiche per creare relazioni interpersonali di varia natura e spesso a contenuto economico.

I metaversi appaiono come mondi virtuali in cui l'individuo opera attraverso un simulacro digitale per poter interagire con gli altri. Riveste particolare importanza l'aspetto legato all'identità personale. Prendendo spunto dal caso Second life, si analizzano: la figura dell'avatar, le diverse attività che un soggetto può svolgere nel metaverso, il rapporto metaverso-diritto, gli ambiti ed i settori giuridici coinvolti, le tutele. Vengono analizzati anche alcuni casi giurisprudenziali emblematici.

L'intento perseguito è dimostrare come ambienti apparentemente innocui e comunque lontani dalla realtà di tutti i giorni siano, invece, destinati a diventare luoghi di grande utilità, ottimi sia per la formazione (in ambiente scolastico in genere ed universitario in particolare, attraverso il potenziamento del più conosciuto *e-learning*) sia per la sperimentazione di nuove forme di commercio elettronico. In entrambi i casi le regole giuridiche, praticamente assenti fino ad oggi, diventano necessarie e la presenza del giurista importante.

GUIDO DI DONATO

La rete aperta: riflessioni sui valori e le regole dell'innovazione 2.0

The Open Network: Values and Rules of Web 2.0

The proliferation of the electronic communications network during the last decade has connected persons, places and ideas in ways which are unprecedented throughout history, as well as heightened the evolution of knowledge, of social structures, of new models of economical innovation and transformation, all based on the opportunity given to go beyond physical and geographical boundaries.

From this point of view, the Author analyzes the most relevant aspects of social and cultural changes, which issue from the evolution of IT, focusing in particular on the study of internet platforms and the related perspectives of scientific, economical and legal innovation.

The essay, through an ingenious theoretical process, retraces the significant changes that the digital revolution is determining on the entire country (from the organization of businesses to that of public opinion, growingly involved in the process of democratic participation) and identifies the technological and infrastructural variables (*Next Generation Network*) as the principal means of re-enhancing productivity, essential for overcoming the present economic situation.

In the same path, the paradigm of *open collaborative innovation* is seen as the key to establish a new productive ecosystem which includes the creation of science, art, law and in a general consideration, the construction of a new pattern of horizontal culture for social development. The new *open innovation* model is based on cooperation processes and common goals – whose development is mainly based on the contributions of the users linked to the web's *ideagorà* – as well as on the activities of less structured groups which operate without a management and beyond hierarchies or traditional forms of organization (*organizational autopoiesis*).

This enormous creative potential, located well beyond the boundaries of companies, universities and Nations, represents the "global brain" which generates innovation strategies based on the web and the sharing of information (*peering*).

The notion of firm itself so becomes one of the few phenomena of civil law which can be rebuilt on the web, or to be more precise a transversal integration system which allows to conjugate a plurality of players and interests.

* * * * *

La proliferazione delle reti di comunicazione elettronica nel corso dell'ultimo decennio ha connesso persone, luoghi e idee con modalità che non avevano precedenti nella storia, ma ha anche catalizzato l'evoluzione della conoscenza, delle strutture sociali, di nuovi modelli di innovazione e trasformazione economica, basati sulla libertà di trascendere confini fisici e geografici.

In questa ottica, l'Autore analizza gli aspetti più rilevanti dei mutamenti sociali e culturali, scaturiti dall'evoluzione delle tecnologie dell'informazione, dedicando particolare e mirata attenzione allo studio delle piattaforme internet ed alle connaturali prospettive di innovazione scientifica, economica e giuridica.

Il saggio, attraverso un'originale ricostruzione teorica, ripercorre le profonde trasformazioni che la rivoluzione digitale ha determinato anche a livello di sistema paese (dall'organizzazione delle aziende a quella dell'opinione pubblica, coinvolta nel processo di partecipazione democratica alla vita delle istituzioni) ed identifica nelle variabili tecnologiche e infrastrutturali (*Next Generation Network*) i principali *riabilitatori* di produttività, necessari al superamento dell'attuale congiuntura economica.

In questa traiettoria, viene altresì incardinato il paradigma dell'*innovazione aperta o collaborativa,* quale chiave di sintesi per l'affermazione di un nuovo ecosistema produttivo che ricomprende la produzione di scienza, arte, diritto e più in generale di *pattern culturali orizzontali* funzionali a nuove forme sviluppo sociale. Il modello di innovazione proposto è caratterizzato da processi cooperativi ed oggetti condivisi – la cui valorizzazione è incentrata prevalentemente sui contributi partecipativi e di condivisione degli utenti connessi all'*ideagorà* della rete – nonché dall'azione di gruppi poco strutturati che operano senza direzione manageriale e al di fuori di logiche gerarchiche o di organizzazione istituzionale (*autopoiesi organizzativa*).

Questo vasto potenziale creativo, collocato oltre i confini delle aziende, delle università, degli Stati, rappresenta la *mente globale* che genera stra-

tegie di innovazione centrate sulle reti e sulla condivisione di informazioni (*peering*).

La nozione stessa di impresa si trasforma così in uno dei pochi fenomeni di diritto privato riscostruibili in termini di rete, ovvero un sistema di integrazione trasversale che consente di coniugare una molteplicità di attori e di interessi.

GIOVANNI PELLERINO

I rischi del diritto nella Rete globale

Risks of Law in the global Network

After analyzing some critical points of legal system in the modern technological age, the author tackles certain questions raised by the legal system's description and representation of itself and its capacity to identify the elements of continuity and of breakage between the lex mercatoria and state law. His reasoning starts with a review of juridical paradoxes as enshrined in Niklas Luhmann's systems theory.

As a result of his analysis, the author then suggest the need to redefine some assumptions of Illuministic conception of the state of law and proposes to consider the issues related to internet's legal treatment as a stage of the legal system's evolution.

* * * * *

Dopo aver analizzato alcuni punti critici del sistema giuridico nell'era tecnologica moderna, l'autore affronta alcune questioni sollevate dalla descrizione del sistema giuridico, dalla sua rappresentazione e dalla sua capacità di individuare gli elementi di continuità e di rottura tra la lex mercatoria e la legge dello Stato. Il suo ragionamento parte da un'esame dei paradossi giuridici sanciti nella teoria dei sistemi di Niklas Luhmann.

Come risultato della sua analisi, l'autore suggerisce la necessità di ridefinire alcuni presupposti della concezione illuministica dello stato di diritto e propone di considerare le questioni relative al trattamento giuridico della Rete come una tappa del processo evolutivo del sistema giuridico.