ASPETTI GIURIDICI DI INTERNET

Contributo ai lavori del

Internet Governance Forum

sommario editoriale a cura di

STEFANO TRUMPY

PRESIDENTE SOCIETÀ INTERNET - CAPITOLO ITALIANO DI ISOC

INDICE

SOMMARIO EDITORIALE

STEFANO TRUMPY

ISOC NASCE COME L'ASSOCIAZIONE DEGLI "OLD BOYS"

Internet assume l'attuale nome nel 1990 quando ancora era una rete conosciuta prevalentemente nel settore accademico e di ricerca nota con il nome ARPAnet; la Internet SOCiety (ISOC) viene costituita nel 1992 con il contributo dei pionieri tecnici della rete, quelli indicati nel titolo del paragrafo come gli "old boys". Sono orgoglioso di avere portato l'Istituto CNUCE del CNR, che ho diretto dal 1983 al 1996, tra i membri organizzativi che fondarono ISOC, così come Enzo Valente, allora Direttore del CNAF, fece per lo INFN.

A QUESTI SI AGGIUNGONO I LEGALI, SOCIOLOGI, ETC.

Nel primo quinquennio la rete Internet si afferma progressivamente, restando tuttavia relativamente marginale nel panorama globale delle reti per trasmissione dati e condivisione di applicativi. Si usa identificare il 1995 come l'anno in cui Internet si afferma come la futura rete globale; il numero degli utenti a livello mondiale aumenterà esponenzialmente negli anni successivi. Poiché la rete viene a costituire una risorsa che coinvolge sempre più larghi strati della società civile, ecco che, accanto ai così detti "teckies" (i tecnici in grado di occuparsi della gestione, degli sviluppi del sistema rete e delle applicazioni in essa contenute) si affacciano nuove categorie di figure professionali che contribuiscono allo sviluppo ordinato - per quanto possibile - della rete stessa. Tra queste categorie, che includono professionisti dell'informazione e dei media, sociologi, governanti e utenti, quella dei legali è una delle più significative. Infatti, man mano che l'utenza aumentava, coinvolgendo strati diversi della popolazione, ed aumentavano le applicazioni disponibili sulla rete, fioriva anche un potenziale contenzioso a vari livelli, inclusi quelli legislativi e relativi ad accordi internazionali necessari per limitare le "patologie della rete". Si veda, a proposito di questa definizione, l'articolo "Fisiologia e patologie della rete" che ho pubblicato insieme all' amico Giorgio Giunchi nel Quaderno "La rete contro lo spam: che cos'è, come combatterlo" disponibile a http://www.quadernionline.it. Il chapter italiano di ISOC veniva creato nel 2000 e sin dall'inizio è stata costante, tra i soci individuali, la presenza di legali interessati a mescolarsi con noi tecnici per capire l'evoluzione di una realtà complessa come il sistema Internet; i loro contributi sono stati preziosi, anche per noi tecnici, per allargare la visione d'insieme del sistema.

LA SOCIETÀ DELL'INFORMAZIONE E LA CRESCENTE INTERDISCIPLINARIETÀ DEL SISTEMA INTERNET

Ormai da alcuni anni si parla di "Società dell'Informazione" per individuare la fase storica nella quale viviamo, vista come fase del progresso civile o, se vogliamo, dell'era industriale dell'umanità. Le Nazioni Unite hanno organizzato due Summit (World Summit on Information Society) che si sono svolti a Ginevra nell'autunno 2003 ed a Tunisi nell'autunno del 2005. Significativo è in particolare il secondo Summit di Tunisi, nel quale si sono raggiunti risultati faticosamente negoziati tra i paesi più sviluppati e quelli in via di sviluppo. Per quella occasione ISOC Italia realizzò un Quaderno sul "Futuro della Gestione Internazionale di Internet", che riporta le discussioni internazionali sul tema ed è disponibile a http://www.quadernionline.it/. Il Summit di Tunisi ha prodotto due risultati concreti:

1. La definizione della così detta "enhanced cooperation" che prefigura il compimento della internazionalizzazione della gestione del sistema di indirizzi della rete Internet (DNS= Domain Name System) oggi ancora supervisionato dal governo degli USA;
2. un piano quinquennale per lo IGF (Internet governance Forum) che discute annualmente i temi della "governance" intesi in senso allargato e quindi che comprendono anche l'aspetto dei contenuti e quelli legati alla infrastruttura di rete.

ISOC E LO INTERNET GOVERNANCE FORUM

Il primo dei due punti citati sopra è il terreno di azione di ICANN (Internet Corporation for Assigned Names and Numbers), che gestisce appunto il sistema di indirizzi di Internet per permettere alla rete stessa di conservare la propria unicità e globalità di accesso. ICANN è legata da un Joint Project Agreement (JPA) con il Dipartimento del Commercio del governo degli USA; il JPA andrà a scadenza nel Settembre 2009; per quella data si presuppone che il JPA non verrà rinnovato e questo sarebbe un ulteriore passo nella direzione della internazionalizzazione della gestione del DNS; preciso anche, nella mia funzione di rappresentante del governo italiano nel Governmental Advisory Committee di ICANN, che già oggi ICANN è gestita con criteri internazionali e che l'intromissione del governo USA nella gestione è minima, e comunque in affievolimento. Il processo della "enhanced cooperation" prefigura una situazione nella quale le entità internazionali come ICANN, ISOC e le organizzazioni ad essa connesse tra le quali lo IETF (Internet Engineering Task Force) che sviluppa gli standard di Internet, W3C che sovrintende allo sviluppo della tecnologia WWW, le entità intergovernative come lo ITU (International Telecommunications Unit delle Nazioni Unite), WIPO (World Intellectual Property Rights) ed altre collaborino tra loro per una evoluzione che veda tutti gli Stati in grado di dare il loro contributo

nella gestione del sistema degli indirizzi di Internet, su base paritaria. Va precisato che ISOC ha un forte legame con ICANN per due motivi fondamentali: ISOC, in associazione con un grosso provider, è responsabile del registro ".org" ed inoltre i chapter di ISOC rappresentano un asse portante della così detta "at large community" di ICANN. È facile comprendere che ISOC ha un ruolo importante da giocare in ambito IGF, indipendentemente dai propri legami con ICANN. Lo scorso anno i temi principali discussi nello IGF di Atene sono stati:

1. OPENNESS 2. SECURITY 3. DIVERSITY 4. ACCESS

Questi 4 temi sono stati confermati nell'agenda di Rio dove - dal 12 al 15 novembre 2007 - si svolgerà il prossimo IGF. I temi in questione sono da sempre all'attenzione di ISOC e per questo motivo ISOC.org, la nostra "casa madre", è mobilitata per una partecipazione attiva allo IGF.

IL PROSSIMO IGF DI RIO E LA SUA AGENDA

In aggiunta ai temi trattati ad Atene, su iniziativa del governo ospitante del Brasile, ci sarà anche un punto aggiunto relativo alle così dette "critical resources" che includono il DNS ed il "root server system"di Internet. La giustificazione di questa aggiunta è collegata al fatto che il processo della "enhanced cooperation" non è stato formalmente avviato da parte del Segretario Generale delle Nazioni Unite e pertanto alcuni paesi, oltre a fare pressioni presso il S.G. affinché lo attivi, chiedono che delle "critical resources" si parli nel prossimo IGF, pur essendo il forum un consesso ove si discute ma non si negoziano testi di risoluzioni. La posizione del nostro governo è che va bene che si parli del tema aggiunto ma che, qualora il processo della "enhanced cooperation" venisse lanciato, questa parte della discussione sarebbe un'inutile duplicazione entro lo IGF. È Rilevante il fatto che ICANN sarà presente a Rio ed anche che ci sarà una rappresentanza del GAC, per dimostrare quali passi siano in corso nella direzione della internazionalizzazione della gestione del DNS. ISOC sarà quindi presente e preparata ad intervenire su tutti i temi; per questo ISOC ha deciso di organizzare la sua presenza anche attraverso un gruppo di persone dedicate al Forum, che verranno selezionate per svolgere la funzione chiamata "ISOC IGF Ambassadors Program". Questo dà un'idea di quanto importante sia per ISOC lo IGF.

I CHAPTERS DI ISOC E LO INTERNET GOVERNANCE FORUM

Innanzitutto il nostro chapter: la predisposizione di questo Quaderno è intesa come un sostanziale contributo per sensibilizzare la nostra comunità Internet sui temi discussi nello IGF. In occasione dei passati Summit e dello scorso IGF, abbiamo notato poca attenzione da parte dei media italiani e poco interesse da parte della comunità degli utenti e dei prestatori di servizi. Comprendiamo bene che in questi incontri internazionali non si prendono decisioni concrete che influiscono in tempi

brevi sul mercato o sulle opportunità di utilizzo della rete ma, ad ogni modo, segnaliamo che si introducono delle tematiche che avranno un'influenza a medio e lungo termine su un sistema di servizi che interessa tutti; pertanto riteniamo particolarmente utile questa azione di sensibilizzazione. In aggiunta, ISOC Italia è tra i promotori della "dynamic coalition: Internet Bill of Rights", assieme ai governi di Italia e Brasile. Le "dynamic coalitions" sono gruppi di organizzazioni, formatisi ad Atene, che si sono impegnati a portare avanti, con continuità, delle tematiche specifiche. Il nostro governo, in preparazione del forum di Rio, sta organizzando un meeting internazionale a Roma per il 27 settembre sul tema: "Dialog Forum on Internet Rights". Il tema in questione tocca in modo orizzontale i 4 temi che si sono discussi ad Atene; i proponenti, tra i quali spicca la personalità di Stefano Rodotà, quale opinion leader per parte italiana, intendono definire un protocollo di diritti (e conseguenti doveri) che rappresenti le regole del buon vivere in Internet accettate da tutti. Faccio notare a questo proposito che ad alcuni osservatori non è piaciuto l'utilizzo della parola "bill", che lascia intendere una natura legislativa vera e propria come scopo dell'attività. Non a caso nel decidere il nome dell'incontro internazionale di Roma si è fatto attenzione a non usarla. ISOC Italia è ben rappresentata nel gruppo di esperti sulla Internet governance, attraverso quattro dei suoi soci (Laura Abba, Vittorio Bertola, Joy Marino e chi scrive), incaricati lo scorso anno dal Ministro Nicolais per la predisposizione delle linee di azione italiane sulle grandi tematiche di Internet. Tutti stiamo attivamente partecipando all'organizzazione della giornata del 27 settembre. Diversi altri chapter hanno organizzato presentazioni e intrapreso attività di sensibilizzazione sullo IGF ed hanno intenzione di partecipare attivamente al meeting di Rio. Tra questi, cito in particolare il chapter francese di ISOC che ha partecipato come partner organizzativo alla pubblica consultazione svoltasi in Francia "Forum des droits sur l'Internet". Il Forum ha prodotto un interessante rapporto di sintesi reperibile all'indirizzo http://www.foruminternet.org/.

L' IDEA DI QUESTO QUADERNO COME SENSIBILIZZAZIONE SUI TEMI DELLO IGF PER LA NOSTRA COMUNITÀ

Per quanto spiegato sopra, si è prodotta una pubblicazione in lingua italiana, se pure gli argomenti sono di interesse globale e si sarebbe giustificata una pubblicazione in inglese da "esportare" anche in altri consessi. A questo aspetto ci pensa ISOC.org, la nostra casa madre, che incoraggia i propri chapter a svolgere attività di promozione e di diffusione nelle lingue locali. Posso comunque testimoniare che, anche a seguito della pubblicazione dei precedenti Quaderni, pure in italiano, ci sono state richieste copie sia da persone che capiscono l'italiano sia da altri che si sarebbero fatti tradurre le parti di loro interesse. Teniamo conto anche che, sotto il tema della diversità discusso nello IGF, uno degli aspetti sui quali si insiste di più è il multilinguismo. Con questo Quaderno

abbiamo l'ambizione di portare un numero maggiore di persone, tra quelli che sono sensibili a comprendere come la rete venga organizzata e gestita a livello globale, ad interessarsi delle discussioni in ambito IGF ed a dare contributi a chi è direttamente coinvolto nelle azioni in corso a livello internazionale.

I TEMI TRATTATI E GLI AUTORI INVITATI

Con le note precedenti ho voluto spiegare le ragioni che hanno mosso ISOC Italia a produrre questo Quaderno. Per iniziare il lavoro, si trattava di scegliere autori sensibili alle tematiche dello IGF e di formazione giuridica. Alcune persone con queste caratteristiche erano già tra i nostri soci - come accennato all'inizio - ma, oltre a queste, abbiamo cercato di allargare l'interesse a personaggi noti e meno noti che hanno svolto attività sui temi descritti. Tra le persone di mia conoscenza, ho avuto la fortuna di interagire con il nostro socio Antonio Anselmo Martino - professore dell'Università degli Studi di Pisa - che conosco da più di venti anni, quando eravamo colleghi direttori di Istituti del CNR, lui all'Istituto di Documentazione Giuridica del CNR ed io all'Istituto CNUCE. Antonio era, a mio giudizio, la persona ideale per svolgere la funzione di curatore di questo Quaderno, per una serie di ragioni: argentino ma full professor di una Università italiana, è rimasto un libero pensatore e docente fuori dalle diatribe nazionali; è un old boy anche lui per gli aspetti che riguardano le normative e le leggi nell'ambito della Società dell'Informazione; avendo diretto un istituto del CNR, ha comunque diverse relazioni in ambito nazionale; infine è una persona piacevole e gentile che si fa ben volere da tutti. Come Presidente di ISOC Italia ed ex collega, ho lavorato molto piacevolmente con lui e confido che apprezzerete i risultati di questa collaborazione. Abbiamo invitato 13 relatori a contribuire a questo Quaderno; sono certo che non abbiamo raggiunto tutti quelli che avrebbero potuto contribuire e che qualcuno sarà forse dispiaciuto di non essere stato invitato a farlo, ma il nostro è stato un best effort. Sono anche convinto che alcuni degli autori non avevano, quando hanno aderito all'invito, una chiara visione delle discussioni in corso nello IGF ma che, dopo il contributo che ci hanno dato, riserveranno maggior interesse al seguito delle discussioni internazionali sulla Internet governance. Qui di seguito sono riportati gli abstract degli articoli che abbiamo raccolto nel Quaderno presentati in ordine alfabetico di autore. Dalla loro lettura si evince come l'insieme delle relazioni offra un rilevante contributo alla discussione che si terrà a Rio. Alcuni degli articoli trattano temi generali che, pur non essendo esplicitamente menzionati nel "menu" di Rio, danno indicazioni assolutamente rilevanti per un quadro di riferimento. Altri affrontano il tema dei Diritti in rete, quello delle Risorse critiche ed i quattro temi già discussi nello IGF di Atene (Libertà di espression, Sicurezza, Diversità e Accesso).

1. DAL DOCUMENTO CARTACEO AL DOCUMENTO INFORMATICO: "DEMATERIALIZZAZIONE"? (MANLIO CAMMARATA)

Dalla carta al bit, dal "faldone" alla memoria elettronica. I problemi che si creano possono essere divisi in due ordini. Il primo è dato dall'imposizione di un cambiamento culturale profondo in tempi troppo brevi. Il secondo ordine di problemi riguarda la normativa, con in più le difficoltà di comprensione reciproca tra giuristi e tecnologi. Il passaggio "dalla carta al bit" è traumatico. I documenti di carta hanno una consistenza fisica evidente. I secondi no: sono "da qualche parte" in un sistema informatico. È un fatto che lo sviluppo dell'e-commerce, dell'e-government e di qualsiasi altra attività con sistemi informatici implica necessariamente la sostituzione dei documenti cartacei con documenti in formato digitale. Questo processo è generalmente descritto come "dematerializzazione" dei documenti. La considerazione, teoricamente corretta, che la falsificazione di un documento informatico è molto più difficile di quella di un documento di carta, non può portare alla conclusione che il primo è "più sicuro" del secondo. Con le attuali norme italiane questa presunzione è molto debole. Insomma, la dematerializzazione può essere un concetto utile, ma deve essere "maneggiato" con i piedi ben piantati per terra…

---

2. SPAMMING E FURTI DI IDENTITÀ (FRANCESCO CELENTANO, GERARDO A. CAVALIERE, MICHELE IASELLI e DAVIDE MERLITTI)

ll fenomeno dello spamming contagia in maniera virale tutta la rete Internet, senza distinzioni di cultura, estrazione sociale, provenienza geografica. Come una beffa tecnologica, in questo campo non opera alcun digital divide: tutti gli utenti della Rete si trovano indistintamente nella posizione di doversi difendere da questi continui attacchi. Le strategie per contrastare la diffusione della posta elettronica non desiderata sono state diverse e proteiformi, ma altrettanto scarse di risultati concreti. Le iniziative a livello internazionale e locale non hanno sortito, nel corso degli anni, gli obiettivi tanto attesi. Il dilagare di questa preoccupante "patologia" della Rete, fra l'altro, è stata "scoperta" anche dalle organizzazioni criminali, che hanno iniziato a sfruttarla per porre in essere mirate truffe on line e cercando di ingannare in maniera più o meno intuitiva il navigatore. Dopo una prima e necessaria introduzione sulla storia della posta elettronica, si affronteranno nell'ordine: le sue peculiari caratteristiche tecniche, le motivazioni che rendono l'uso di questo strumento tanto amato dai navigatori, la nascita dello spamming (le tecniche di realizzazione e gli strumenti utilizzati per l'invio in massa di posta spazzatura, gli strumenti per difendersi dallo spamming, i filtri bayesiani, le Dnsbl, ecc.), Spim (spam attraverso il servizio di instant messaging), Splog (spam attraverso i blog), mail bombing, mail spoofing, phishing, scam (e truffa nigeriana), ecc.

---

3. INTERNET GOVERNANCE E TUTELA DELL'UTENTE IN ITALIA (ENZO FOGLIANI)

Oggi gli utenti della rete sono circa 1200 milioni; circa un decimo di questi hanno un proprio nome a dominio per farsi riconoscere meglio nella posta elettronica e per facilitare l'accesso ai propri siti web. Mentre i gTLD sono gestiti attraverso ICANN in modo uniforme, i ccTLD come il nostro hanno una maggiore autonomia gestionale. Nella prima parte di questo articolo viene illustrato lo sviluppo storico della Internet governance in Italia, descrivendo il precedente sistema basato Registration Authority e Naming Authority e l'attuale sistema accentrato presso il Registro del ccTLD.it. Nella seconda parte sono esaminati gli strumenti, posti dal regolamento per l'assegnazione e la gestione dei nomi a dominio italiani posti a disposizione degli utenti per risolvere, in alternativa al ricorso all'autorità giudiziaria, le vertenze inerenti alla registrazione di nomi a dominio violando diritti altrui. La terza ed ultima parte è dedicata all'esame degli attuali rapporti giuridici che si istaurano con la registrazione di un nome a dominio fra registro, maintainer ed assegnatario, con particolare riguardo alle possibilità di tutela dell'utente nei confronti del registro e del proprio maintainer.

---

4. INTERNET E PUBBLICHE AMMINISTRAZIONI: QUALE DEMOCRAZIA ELETTRONICA? (ANDREA MAGGIPINTO)

Le nuove tecnologie dell'informazione e della comunicazione stanno apportando all'azione delle Pubbliche Amministrazioni (PPAA) elementi di assoluta novità, anche sul piano strettamente giuridico. Rilevante è il ruolo della "communication technology", in grado di realizzare il dialogo telematico tra cittadini, amministrazioni territoriali e organi di governo su tre livelli strategici di interazione: inter-amministrativo (dialogo tra PPAA); inter-soggettivo (dialogo cittadino-PA); politico-istituzionale (dialogo Cittadini-Istituzioni). Per ciascuno di questi livelli vengono evidenziati gli aspetti che necessitano di un rinnovato impegno da parte dei decisori tecnologici: (i) fruibilità dei dati e cooperazione tra PPAA; (ii) accesso telematico e disponibilità dei dati digitali; (iii) trasparenza informatica e partecipazione delle azioni di governo. Diviene ormai indispensabile l'adozione di standard comuni a livello logico - con particolare riguardo alla semantica per la definizione e la gestione concettuale delle informazioni - e di metodologie di cooperazione tra Pubbliche Amministrazioni. Un ruolo importante può essere svolto dalle amministrazioni regionali. Le tecnologie di comunicazione rilevano evidentemente anche nei rapporti tra Cittadini e

Istituzioni. L'espressione "democrazia elettronica" sembra acquisire un nuovo valore universale, che risiede nella realizzazione di una trasparenza informatica dell'azione amministrativa. Il modello teorico dello Stato di diritto - sotto la spinta multidimensionale delle tecnologie dell'informazione e della comunicazione - affronta nuove sfide, prima fra tutte quella di governare il processo di democratizzazione sociale in atto, individuando nuovi modelli sostenibili, inclusivi e realmente efficaci per il riconoscimento dei diritti fondamentali dei cittadini. Il diritto pubblico, anche sul piano internazionale, può rappresentare la via per bilanciare i rischi di un progresso tecnologico non sostenibile. Gli Stati, nel processo sovranazionale di definizione di una governance di Internet, sono chiamati a definire, con razionalità globale, il loro spazio politico.

---

5. INTERNET E DIRITTO D'AUTORE, UNA RELAZIONE NECESSARIA MA TORMENTATA (LAURENT MANDERIEUX)

Il Web ha una relazione strettissima con il tema del diritto d'autore: in effetti, tutti i contenuti messi online sono sottoposti alla tutela del diritto d'autore sotto una forma o l'altra (anche in caso di diritto d'uso completamente libero). Malgrado i tentativi di miglioramento introdotti dalle Convenzioni internazionali (WCT, WPPT), l'interazione con il diritto d'autore rimane tuttora difficile, poiché Internet è di per sé un oggetto di carattere internazionale e i siti di qualsiasi ccTLD o GTLD sono accessibili da qualsiasi computer in qualunque parte del globo, mentre il diritto d'autore rimane governato da ogni Stato sul suo proprio territorio. Il problema è reso ancora più complesso dal divario Nord-Sud: i contenuti di cui i Paesi del Sud necessitano al fine di ridurre il loro gap scientifico e tecnologico sono quasi sistematicamente prodotti nei Paesi del Nord e protetti, talvolta iperprotetti, da questi Paesi. D'altronde, la tecnologia nel Nord del mondo si può sviluppare solo grazie alla protezione della Proprietà Intellettuale. Insomma, per uno sviluppo sano e non liberticida di Internet, bisogna cercare di risolvere, almeno in parte, il conflitto tra gli interessi dei creatori e quelli del pubblico, tema che su cui fece chiarezza già nel 1948 l'Articolo 27 della Dichiarazione Universale dei Diritti Umani dell'ONU: " Ogni individuo ha diritto a prendere parte liberamente alla vita culturale della comunità, di godere delle arti e di partecipare al progresso scientifico e ai suoi benefici. " Ogni individuo ha diritto alla protezione degli interessi morali e materiali derivanti da ogni produzione scientifica, letteraria e artistica di cui egli sia autore. Poiché è favorevole alle libertà degli individui che l'attività normativa sia in ritardo sui fenomeni economici, culturali e sociali, è anche opportuno non legiferare in eccesso o troppo velocemente su diritto d'autore e Internet. Piuttosto sarebbe opportuno promuovere dei meccanismi comportamentali pragmatici (guidelines, voluntary codes, etc.) per alleviare la contrapposizione tra creatori e pubblico:

potrebbero essere individuate soluzioni e vie pragmatiche a livello globale, in parte sviluppate a partire dal modello usato per risolvere le frizioni tra nome di dominio e marchio. Questo non solo per diminuire il divario Nord-Sud ma anche per rendere più fluida anche al Nord la gestione dei diritti d'autore sul supporto "Internet" per i creatori e per tutta la comunità Internet.

---

6. INFOETICA (ANTONIO ANSELMO MARTINO)

L'etica interviene in tutti i rapporti umani, quindi anche nei rapporti che nascono dalle nuove tecnologie. Molte volte è difficile tracciare il limite tra la soluzione giuridica e la soluzione etica, in ogni caso, appunto perché è un campo nuovo, l'etica ha molto da dire nella visione giuridica di Internet. Ad incominciare da come si potrebbero affrontare i temi del divario digitale, del multilinguismo e l'accettazione dell'altro, dei diritti delle maggioranze ma anche di quelli delle minoranze, dell'esclusione di Internet, della tensione tra libertà individuale e sicurezza collettiva in un campo dove praticamente si deve riscrivere tutto. Fin dove può, e sopratutto deve, arrivare il governo in linea. La massimizzazione dell'utilità fin dove è compatibile col rispetto delle pratiche democratiche, della privacy, della tutela del frutto del proprio lavoro. Fino a dove e fino a quanto si deve spingere la sostituzione della volontà cosciente a decisioni automatiche controllate e calibrate? Esiste un diritto alla sicurezza? e un diritto al consumo? Quanto aspetteremo per avere una carta fondamentale dei diritti alla quale corrispondano organismi, imprese o privati obbligati? Proviamo a contestualizzare problemi e soluzioni. Mettiamo a confronto società dell'informazione e qualità della vita.

---

7. INTERNET: QUANDO LE REGOLE "DAL BASSO" PIOVONO "DALL'ALTO" (ANDREA MONTI)

Il potere esecutivo sta deliberatamente sostituendosi al Parlamento nella regolamentazione delle tecnologie dell'informazione. Con la scusa di promuovere "codici deontologici" e "autoregolamentazioni", atti che dovrebbero provenire spontaneamente dal mondo delle imprese ma che in realtà sono a tutti gli effetti controllati da questo o quel ministero, si è creato un regime regolamentare del tutto fuori controllo. Tutto questo è stato possibile per colpa della bieca ignoranza dei politici e, dall'altro lato, dall'incapacità della società civile di reagire a gravi limitazioni dei diritti civili commesse in nome di "interessi superiori" che spesso nascondono derive populiste o ben altre - e meno nobili - "intenzioni".

---

8. TECNICA, DIRITTO, FORMAZIONE E MODELLI COLLABORATIVI (ALESSANDRO NICOTRA)

Per anni Internet è riuscita a progredire su Gentlemen's Agreements ovvero grazie ad un protocollo comportamentale non scritto ma vigente fra tutti i tecnici e gli operatori. A partire dagli inizi degli anni '90 e con il boom di utenti, si sentì l'esigenza di varare una "Netiquette" o galateo della Rete che codificasse, in qualche modo, come ci si dovesse comportare ed interfacciare sul Web. Gli informatici ed i tecnici, in realtà, sono sempre stati abbastanza allergici a qualsivoglia codifica che non fosse segnatamente ed esclusivamente hardware o software. Tutt'oggi giuristi e tecnici si scontrano sovente e sembrano parlare due linguaggi diversi. Sembra una situazione analoga a quando i computer non riuscivano a comunicare tra loro avendo i rispettivi linguaggi e sistemi operativi proprietari. Se il TCP/IP riuscì nel miracolo allora, possiamo aspettarci che questo miracolo di interoperabilità (o multidisciplinarietà, a seconda degli interlocutori) si verifichi oggi che, più che mai, l'Internet di massa richiede anche l'apporto di giuristi specializzati e di norme universali e trasversali? Per farlo è indispensabile investire sulla formazione e sulla inculturazione, una educazione informatica intrecciata alla dimenticata educazione civica. Molti non comprendono che abdicare da un qualsivoglia intervento normativo significa rimetterlo all'arbitrio di legislatori ignoranti e di una classe politica impreparata. Viceversa, adoperando lo stesso modello collaborativo che è alla base della creazione, della diffusione e della libertà dell'Internet, potrebbe essere possibile dopo una diffusa e vasta opera di formazione che le future scelte siano consapevoli e non per tentata imposizione normativa. Perché si deve? Perché dobbiamo. È un imperativo categorico e morale... Kant docet!

---

9. TUTELA DELLA RISERVATEZZA E INTERNET: UN BINOMIO DIFFICILE. IL CASO DELLE INTERCETTAZIONI DELLE COMUNICAZIONI INFORMATICHE O TELEMATICHE (TULLIO PADOVANI)

L'innesto dei mezzi informatici in tutti i centri vitali della società moderna, dal sistema sanitario al sistema bancario, da quello delle telecomunicazioni al sistema commerciale da quello scolastico a quello della difesa, fino all'uso più strettamente "domestico" del computer e di internet ha inciso notevolmente sulla tutela della riservatezza latu sensu intesa. Si tratta, invero, di una rivoluzione del modo di vivere positiva, se si pone a mente al fatto che era inimmaginabile fino a qualche tempo fa poter anche solo pensare di scambiare infinite informazioni in tutto il mondo nel giro di frazioni di secondo, tanto che, oggi, una scoperta effettuata nel posto più disparato della terra, una volta messa

in Rete, diviene patrimonio di tutta l'umanità. Ma, al contempo, presenta anche rovescio della medaglia se taluno si propone di far un uso distorto di questo patrimonio immenso di informazioni sulle cose e sulle persone. La riservatezza trova tutela nell'ordinamento penale che si preoccupa di tutelare la segretezza e la libertà della vita singolo, anche dalle aggressioni informatiche, nel suo domicilio nella sez. IV, del titolo XII, del libro II, del codice penale ("Dei delitti contro l'inviolabilità del domicilio"), e nelle sue comunicazioni, sez. V, del titolo XII, del libro II, del codice penale ("dei delitti contro l'inviolabilità dei segreti"). Tuttavia, tale tutela non sempre appare adeguata all'insidiosità delle recenti forme di aggressione non solo quantitativamente, ma anche qualitativamente nuove, tanto che la stessa nozione di privacy ne risulta significativamente modificata. Si tratta, infatti, di previsioni che non sembrano cogliere nel segno della nuova "emergenza" informatica, stante anche il fatto che ad ormai quasi quindici anni dall'ingresso delle suddette norme nel nostro codice le pronunce sono pochissime, tanto si possono contare sulle dita di una mano, mentre altrettanto non sembra potersi dire per la diffusione della violazione della privacy.

---

10. INTERNET E ANSIA DI SICUREZZA: IL RISCHIO INFORMATICO (GIOVANNI PASCUZZI)

Il diritto dell'era digitale sembra caratterizzato dall'ansia di sicurezza. Senza sistemi informatici sicuri, il diritto alla protezione dei dati personali si svuoterebbe di significato. Sicura si vuole sia la navigazione in rete, specie per scongiurare il pericolo che i minori abbiano accesso a contenuti nocivi o indecenti. Sicuri devono essere i meccanismi di firma, perché alla loro affidabilità è ancorata la certezza dei traffici. Sicure non possono che essere le transazioni sulla rete (si veda il tema dei protocolli per i pagamenti via rete), se il commercio elettronico deve definitivamente decollare. Il contributo si propone di analizzare la nozione di sicurezza e i possibili sviluppi, sul piano giuridico, del rischio informatico.

---

11. SICUREZZA E PRIVACY NELLE COMUNICAZIONI ELETTRONICHE (FRANCESCO PIZZETTI)

Il bilanciamento costituzionale tra le esigenze di privacy e sicurezza costituisce un problema particolarmente avvertito rispetto al mondo di Internet e della rete. Le autorità amministrative nazionali di garanzia si fanno ampiamente carico di queste esigenze sul versante applicativo, come dimostra l'esperienza recente del Garante per la protezione dei dati personali anche in riferimento ai

gestori di servizi di comunicazione elettronica. Inoltre, la richiesta di maggior sicurezza è inestricabilmente legata alla stabilità delle attività commerciali ed economiche intraprese on-line. Le misure di sicurezza previste in quest'ambito dal Codice privacy, se abbinate ad una maggiore trasparenza da parte dei fornitori, risultano, peraltro, in grado di garantire un'alta personalizzazione dei servizi in rete limitando i casi di furto di identità, nel solco di una tendenza ormai ampiamente diffusa a livello internazionale.

---

12. PARLAMENTI E SVILUPPO DELLA SOCIETÀ DELL'INFORMAZIONE (STEFANO RODOTÀ)

Le tecnologie dell'informazione e della comunicazione hanno da tempo imposto una rinnovata analisi del ruolo dei parlamenti, del rapporto tra democrazia rappresentativa e democrazia diretta. La prospettiva da considerare è quella di una trasformazione delle relazioni tra istituzioni parlamentari e cittadini.

---

13. IL DIGITAL DIVIDE E LE TELECOMUNICAZIONI: POTENZIALI SOLUZIONI TECNICO REGOLAMENTARI (FULVIO SARZANA DI S. IPPOLITO)

L'affermazione delle tecnologie dell'informazione sta trasformando profondamente le strutture sociali ed economiche di tutti i paesi collegati alla rete internet . Fra le conseguenze primarie di questa diffusione vi è però la creazione di zone di eccellenza e di veri e propri "ghetti" digitali. Con digital divide si intende il divario esistente tra chi può accedere alle nuove tecnologie presenti in misura sempre più consistente nel mercato, e chi non può farlo per motivi diversi come reddito insufficiente, scarsa o nulla conoscenza della tecnologia, assenza di infrastrutture (come nel caso dei paesi in via sviluppo). Si distinguono tradizionalmente un digital divide verticale, intendendosi in tal senso il divario che esiste tra cittadini di uno stesso paese che, in assenza dei medesimi requisiti di sviluppo, siano di fatto esclusi dai benefici della rivoluzione digitale e digital divide orizzontale, ovvero il divario esistente tra i diversi Paesi collegati alla rete in ragione di requisiti economico-sociali che non ne consentono uno sviluppo armonico. Peraltro esistono alcuni casi nei quali le due forme di digital divide possono coesistere, in ragione di una ineguale distribuzione delle infrastrutture di telecomunicazione sul territorio, come accade in Italia. La realtà italiana testimonia come il divario digitale possa riscontrarsi anche in un paese ad elevata alfabetizzazione e con un discreto livello medio di benessere. Condizione necessaria per l'assorbimento o la diminuzione di entrambe le forme di divario digitale è la creazione di una infrastruttura tecnologica in grado di

supportare le comunicazioni in banda larga. Lo sviluppo della banda larga costituisce un fattore d'importanza strategica per il miglioramento delle comunicazioni tra i cittadini, per l'affermazione di competitività delle imprese italiane, al pari della creazione di una rete di trasporti autostradale e ferroviaria più efficiente. Il contributo analizzerà gli strumenti regolamentari e le esperienze concrete ritenuti più utili al superamento del digital divide.

RINGRAZIAMENTI

Ringrazio, prima di tutti, i soci e i sostenitori di ISOC Italia, che con i loro contributi permettono all'associazione di finanziare l'iniziativa dei Quaderni dell' Internet italiano. Desidero esprimere tutta la mia gratitudine ad Antonio, che ha curato il Quaderno; senza la sua presenza difficilmente avremmo potuto realizzare questo lavoro. Grazie anche agli autori che hanno prodotto ottime relazioni, seppur costretti a lavorare in tempi stretti. Un particolare ringraziamento va a Laura, per il tempo dedicato al coordinamento redazionale; preziose sono risultate le sue indicazioni, dalle quali il curatore ed io siamo stati costantemente guidati nell'elaborazione di questo Quaderno.

PREMESSA

ANTONIO ANSELMO MARTINO

Antonio Anselmo Martino, dottore in Legge e Scienze Sociali (ph. D); dal 1983 al 1992 è direttore dell'Istituto per la documentazione giuridica del Consiglio Nazionale delle Ricerche con sede in Firenze. Dal 1981 al 1987 è professore di Scienze Politiche al Corso di Stato Maggiore delle tre forze armate italiane. Dal 1987 al 1993 è Presidente del FIRILITE (Federation of International Research Institutes on Law and Information Technology in Europe). Dal 1970 al 1976 è Professore di Introduzione al Diritto presso l'Università di Buenos Aires e di Filosofia del Diritto presso l'Università dell'Haute-Normandie dal 1977 al 1979. Membro della Commissione Informatica per la rete degli organi del CNR dal 1986 al 1993. È stato Membro della Commissione Scientifica delle seguenti riviste: Del derecho industrial, Buenos Aires; Computer/Law Series, Amsterdam; Artificial Intelligence and Law, Boston; Law and Information Technology, Oxford; Derecho de la alta tecnologia, Buenos Aires. Curatore della collezione Logica, Informatica, Diritto della CEDAM. Attualmente è Professore di Scienza Politica presso la Facoltà di Scienze Politiche dell'Università degli Studi di Pisa; Membro dell'Associazione Italiana di Intelligenza Artificiale; Membro corrispondente dell'Academia Nacional de Derecho y Ciencias Sociales di Cordoba; Membro associato del Center for Artificial Intelligence and Cognate learning of the University of Greenwich; Direttore del Master in Scienza della Legislazione promosso dalle Università di Pisa e del Salvador, nella facoltà di Ciencias Jurídicas de la Universidad del Salvador en Buenos Aires; Direttore del Manual del Digesto Juridico Argentino; Membro del WE/EB-MD8 (EDIFACT Message Developmen Group Legal); Direttore dell'Istituto Internazionale di Studi e formazione su Governo e Società promosso dalle Università di Pisa e Salvador a Buenos Aires; Membro de la RCLS (Research Committee of Legislative Specialists) USA; Direttore Scientifico della Scuola di Alti Studi per il Mercosur, con sede a Montevideo.

"Parleransi e toccheransi e abbracceransi
li omini, stanti dall'uno all'altro
emispherio, e intenderansi i loro
linguaggi"
[Leonardo Da Vinci, Codice Atlantico Profetie]

INTERNET È UN'ANARCHIA CHE FUNZIONA ?

Il presente Quaderno tratta dei temi giuridici, di practicies sociali e di public policy governative sul Governo della Rete, con riferimento a quello che sarà oggetto di attenzione nel Internet Governance Forum (IGF). Ovviamente questo riferimento ad uno specifico appuntamento nulla toglie alla pretesa doppia di fare un quadro dello stato dell'arte, particolarmente in Italia e alla pretesa di dare un orientamento, possibilmente europeo, se si può arrivare a delle conclusioni e raccomandazioni.

Questo Quaderno deve essere essenziale, quasi laconico per la quantità e importanza dei temi da trattare.

Esiste una strana credenza, quasi magica e molto ingenua per la quale Internet funziona così, per arte del caso, grazie all'anarchia. Questa credenza è totalmente priva di fondamento. L'anarchia, per definizione, non funziona. Internet funziona sostanzialmente perché si seguono delle regole. In primo luogo regole tecniche per i collegamenti, le forme dei messaggi e tutti i livelli di sicurezza, completezza e integrità che i messaggi devono rispettare. Questa è la parte più prettamente sintattica, perché vincolata al funzionamento delle macchine che è fondamentale, nel senso primitivo del termine, ma del quale non ci occuperemo.

Vi sono altre regole che riguardano i comportamenti umani volti a dare un'organizzazione minima senza la quale la Rete non potrebbe funzionare. Di queste ci occuperemo noi, non nella loro totalità che esula da un modesto Quaderno, ma nella parte che riteniamo rilevante nell'attuale dibattito internazionale sull'argomento. Le regole sociali hanno non solo un aspetto sintattico, ma anche semantico - come vedremo subito - e sostanzialmente pragmatico; le regole hanno un solo destino: essere adempiute.

LA GOVERNANCE

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 [1] .

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 - e così rafforzare 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 delle amministrazioni necessarie per far fare ai cittadini e alle imprese le azioni che abbisognano per compiere i propri fini. Quindi, la "governance" è positiva, come la governabilità e si verifica quando queste azioni amministrative tendono alla semplificazione e alla qualità, per esempio rendere più facile, più accessibile, più trasparente, più rapido l'ottenimento di un'informazione, la richiesta di un certificato, le autorizzazioni e sopratutto l'interazione con l'amministrazione in quelle azioni più complicate che hanno bisogno dei due attori. In Toscana si sente spesso "rigovernare la tavola", "rigovernare la casa" e persino "il fattore è andato a governare i buoi".

Queste azioni, molto lontane dalla parte celebrativa e fotografica del potere, sono fondamentali per poter permettere di realizzare poi tutte le cose che si devono fare nella casa o nel podere. In un modo semplice potrebbe essere presa come una buona definizione di governance "tutte quelle azioni che deve fare il detentore del potere per permettere alle persone e alle imprese di svolgere la propria azione nella società". Sostanzialmente si tratta di regole giuridiche ma, dato l'attuale orientamento della dottrina in materia politica e sociale, non abbiamo alcun ritegno in trattare le practices sociali e gli indirizzi politici che dai diversi paesi vanno verso la Rete e viceversa. Intendiamoci, ogni pratica sociale, e tale dovrebbe poter essere enunciata con parole, è una regola sociale.

Non vogliamo però immischiarci in problemi di definizioni e demarcazione di territorio normale tra le scienze e dentro le scienze sociali. La stessa parola "Governance" che adopera il titolo del Forum potrebbe essere oggetto di un dottorato di ricerca in Scienze politiche. In italiano vi sono grosse resistenze - condivise - a tradurre governance in "governo" per le molteplici accezioni che questa parola ha nella politica italiana. Gli spagnoli se la cavano molto bene con "gobernanza", diversa da "governo" e da "governabilità" [2].

INTERNET E LA POLITICA

Internet è una rete di reti poco strutturata, ma altamente pervasiva. Ormai non vi è parte della vita sociale e anche individuale dove non vi sia entrata. Ovviamente non ne può fare a meno la politica. Cominciò Al Gore, quando era vicepresidente di Clinton, ad aprire un portale presso la Casa Bianca dove offriva notizie e chiedeva l'interazione del pubblico.

Molti di noi abbiamo partecipato a quella epoca mitica nella quale la Casa Bianca ti rispondeva in una settimana. In poco tempo furono intasati da messaggi e cominciarono a filtrare, e ulteriori filtri durano fino ad oggi. Praticamente oggi tutti i sistemi politici hanno un loro portale come quasi tutti i partiti politici. Per le elezioni queste azioni si moltiplicano. Nel mese di luglio di questo anno c'è stata un'importante esperienza nelle elezioni primarie nordamericane: per due ore i candidati a presidenti democratici sono stati sottoposti a video domande prese da YouTube e diffuse in diretta dalla CNN.

Intendiamoci, non è per niente democrazia diretta, perché le domande venivano filtrate da Anderson Cooper della CNN. David Borman della catena televisiva ha detto di aver curato che lo show non degenerasse in farsa, ma "sentirete domande che noi giornalisti non sappiamo fare". Sfida Zach Kemp, un ragazzo biondo di Utah, mentre la sua faccia riempiva uno schermo gigante di televisione. "Siate onesti. Che cosa farete di diverso dagli altri politici a Washington? Cosa vi farà più efficaci degli altri che promettono e non adempiono?" I candidati hanno provato a difendersi. Hillary Clinton, Barack Obama, John Edwards e gli altri 5 pre candidati democratici hanno dovuto

rispondere a domande che per la prima volta, con video fatti in casa e messi su Internet YouTube, essi avevano in diretta.
La madre di un soldato domanda "quanti ragazzi devono morire ancora prima che i democratici cessino di dare priorità alla politica al di sopra delle loro coscienze, con riferimento all'Irak". Per carità non si tratta di democrazia diretta [3] né molto meno, però è un mezzo attraverso il quale molti possono arrivare a quei pochi che devono decidere o che si presentano in lizza per governare. La circolazione delle idee e uno spazio per la discussione sono il primo tassello di un'organizzanda democrazia diretta. Internet lo può iniziare, con luci ed ombre. Il mezzo è molto potente e questo rende il suo studio serio un imperativo. Tutte le cose che sono possibili tecnologicamente devono essere fatte? Quali i criteri per scegliere?

LA POLITICA IN INTERNET

È in termini politici un problema di poteri: chi fa le regole, come le fa, cercando quali obbiettivi, chi le interpreta per l'applicazione, quale diritto è applicato, chi e l'autorità dirimente se ci sono conflitti, chi controlla i controllori. In altri termini i problemi toccati da questo Quaderno sono molto simili a quelli costituzionali: una costituzione ha due parti: una necessaria, relativa alla distribuzione dei poteri, le facoltà e le giurisdizioni; l'altra, non necessaria, però più importante: la dichiarazione dei valori che saranno sostenuti e che sorreggeranno tutta la struttura giuridica. Se volete, la dichiarazione dei diritti fondamentali.
Ebbene, tutte e due le parti sono discusse in questo momento e fanno parte del Quaderno: chi fa le regole di Internet, come le fa, quali sono gli applicatori e i controllori, quali gli obbiettivi che si devono prefiggere al fine di arrivare a soluzioni universali, generalmente accettate e che facciano funzionare al meglio la Rete. Alcuni problemi affondano le loro radici nella più antica tradizione giuridica. E qui una prima avvisaglia: se Internet è planetaria vi sarà una pluralità di culture giuridiche in competizione - quindi le soluzioni devono tener conto dei contesti e delle consuetudini.
Per questa ragione il primo diritto ad affermarsi in Internet è quello relativo ai mercanti, la lex mercatoria. Perché tutti la adoperano prima e senza Internet. Ma la Rete ha creato nuove situazioni che vanno affrontate anche in questo campo, come per esempio la legge e la giurisdizione applicabile. All'inizio ci muovevamo molto con la Convenzione di Vienna del 1980 relativa alla compravendita internazionale. Dopo, le imprese (sopratutto nordamericane, che sono quelle che più uso fanno del commercio elettronico) hanno incominciato a capire che imporre la propria legge e la propria giurisdizione al compratore costituisce per loro una sicurezza a patto che si mantenga un monopolio. Non appena le prime imprese (minori, alcune piccole imprese) hanno incominciato ad

offrire l'applicazione delle leggi e la giurisdizione del compratore, questo non ha avuto dubbi, anche con sovrapprezzo si sentiva più tranquillo comprando in queste condizioni.
Oggi possiamo dire che la legge ferrea del mercato ha trasformato quelle eccezioni in regola e sono eccezionali invece le imprese che impongono la loro legge e la loro competenza. Questo però ha provocato una discriminazione tra paesi, ingiusta dal punto di vista dell'eguaglianza ideale, ragionevole di fronte ai comportamenti concreti. Una clausola che vediamo spesso dice che il prodotto tale non si venderà nei paesi X, Z o W. Ed è ragionevole che, se un paese non ha leggi stabili né tribunali affidabili, i mercanti non si fidino e quindi non vendano lì. Credito viene da "credere" e sempre di più trionfano quelle comunità e quei settori dove la parola ha un senso, nonostante i vantaggi innegabili delle firme digitali e quant'altri requisiti possibili.

IL GOVERNO DELLA RETE

Chi detta le norme di organizzazioni (costitutive o costituzionali) di Internet e come lo fa è oggetto di dibattito: per la storia particolare di questa rete, il Dipartimento del Commercio degli USA è uno di questi fautori e controllori; poi è nato interesse da parte di altre organizzazioni, sopratutto di tipo intergovernativo, nelle quali hanno rappresentanza tutti i governi. Vi è una via intermedia che considera che le cose si metteranno pian piano d'accordo tra i paesi ma non escludendo il servizio privilegiato degli USA perché altrimenti ogni cambiamento significherebbe una dura battaglia.
E la cosa più importante è mantenere il funzionamento, la diffusione e la crescita della Rete. Internet è una rete di reti; per questo la si chiama "la madre di tutte le reti" o "la Rete" con maiuscola. Tutta Internet funziona grazie al fatto che vi sono 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 l'ICANN, ISOC, WIPO e ITU. Su questi attori e sui rappresentanti dei governi nazionali gira la possibilità di intervenire per fissare i criteri che consentono alla Rete di funzionare, attraverso la migliore collaborazione degli enti citati. 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. 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, ma che allo stesso tempo reggono alle dure repliche della storia (nel dire di Hegel).
Se per un paese è difficilissimo trovare "l'interesse comune", immaginiamoci per una comunità globale. Qui gli attori sono l'Unesco, l'Internet governance Forum dell'Onu, l'OECD, il W3C, oltre ai già citati. Ma potremmo generalizzare a molte delle associazioni nazionali che si occupano del

tema specifico delle regole in Internet e più largamente a tutte le organizzazioni giuridiche e mi spingerei a dire ai giuristi che sono interessati a questo nuovo diritto che le nuove tecnologie hanno fatto nascere. E i temi che devono essere trattati sono tutti i temi che hanno un sottratto giuridico e hanno a che fare con Internet.

Ad esempio, una riunione di pedofili in Second Life è delitto? In caso affermativo, dove? Giudicato con quali norme? Ma anche: cosa devo conservare dei miei dati bancari per avere diritto alla restituzione se c'è un hacker? Quale la responsabilità civile della banca? Con quali prove posso provare un trasferimento elettronico di fondi?

Tutti gli interventi sul diritto in Internet hanno un aspetto altamente tecnico, quindi conviene non intervenire senza una previa consultazione con esperti nel settore. Se si considera la normativa introdotta nella finanziaria italiana destinata a "Rimozione dei casi di offerta in assenza di autorizzazione attraverso rete telematiche che si applica ai fornitori di connettività nella Rete", lo scopo della legge è impedire a chi non ha ricevuto autorizzazione dell'Amministrazione Autonoma di Stato avere siti per giocare on-line. A tal fine l'Amministrazione fornisce un elenco di siti che i provider di accesso devono filtrare e rendere inaccessibili cambiando il record di registrazione nell'area indirizzi (domini), ma l'unico modo di rendere invisibile un'informazione autoritativa è quella di impedire l'accesso (via indirizzi IP filtrati) ai nomi assegnati dai registri autorizzati e in questo modo il "filtro IP" impedisce l'accesso ad interi server che sono autoritativi per centinaia di altre destinazioni; è quindi inattuabile perché oscurerebbe centinaia di altri servizi oltre a quello che si intende realmente oscurare [4], come sostiene l'Associazione ISOC Italia.

Nel ventunesimo secolo non c'è spazio nella governance nazionale per sbagli di tipo tecnico tali da rendere inattuabile una norma giuridica. Il legislatore non ha più quei margini di tempo che in passato consentivano di rimediare a degli errori anche grossolani. La velocità è una parte integrante importante della nozione di Società dell'Informazione e questo implica dei limiti di tolleranza al fallimento sia da parte pubblica che privata o della società civile.

LE REGOLE GIURIDICHE DI INTERNET

Il tema centrale è costituito dalle regole, quali contenuti devono avere? chi le fa adempiere?. E se non vengono adempiute quali sono le sanzioni? Anche in questo campo si pretende normalmente di far scegliere tra soluzioni contrapposte. Questo sembrerebbe veramente facile. Invece, le scelte bisogna trovarle nell'universo dei grigi che vanno da una soluzione molto scontata ad un'altra, opposta, altrettanto scontata con una miriade di possibilità intermedie che sono - generalmente - quelle più attuabili.

Trattandosi di un fenomeno globale [5] esso comporta molti problemi di contestualizzazione del diritto e internazionalizzazione - là dove possibile - di esso. La lex mercatoria è un buon esempio,

ma il diritto si evolve velocemente per forza delle trasformazioni sociali e delle nuove tecnologie non solo nel diritto commerciale, ma anche in quello amministrativo e man mano in una zona intermedia che va cancellando i vecchi confini tra il pubblico e il privato, come ad esempio i diritti del consumatore. Internet ha una sua storia che ha determinato - come spesso avviene nei sistemi giuridici - una forma di governo e un modo di governare.

Contemporaneamente, l'allargamento a mezzo di comunicazione universale di ciò che era nato come una rete accademica, comporta tanti e così profondi cambiamenti che vale la pena interrogarsi su dove siamo e l'immancabile pretesa di sapere dove vorremo essere. Il multilinguismo è un fatto e più paesi sono impegnati massicciamente, più impellente diventa il problema. Il multilinguismo non può essere evitato e contemporaneamente vanno trovati i mezzi di inserimento per la vasta gamma delle lingue parlate in Internet.

Un altro problema non piccolo consiste nel dare un trattamento giuridicamente corretto alle nuove figure che attraverso Internet nascono: i provider, gli host, le pagine web, i blog. E come catalogare con le vecchie teorie i nuovi problemi? Per esempio: c'è un delitto informatico? Nel caso affermativo, quale è il bene giuridico protetto? O piuttosto deve parlarsi dei vecchi delitti che ora sono fatti attraverso la rete, come la truffa del phishing, etc. Ma senza menar il can per l'aia, i temi impellenti continuano ad essere: chi governa Internet? con quale tutela? con quale possibile o probabile sbocco? i rapporti delle politiche nazionali e sopranazionali come si esprimono? e quale effetto hanno sull'interlocutore privilegiato che è il governo della Rete? In mezzo ci stanno una miriade di temi che nascono appunto da questa situazione nuova di un mezzo che salta le frontiere e che mette in discussione il già maltrattato tema della sovranità nazionale.

Un'alzata di scudi di sovranità nazionali farebbe finire Internet, ma Internet ha dei mezzi tecnici per perforare lo scudo delle sovranità nazionali. Si deve trovare un accordo: è un caso curioso di forze opposte di diversa natura che non si possono equilibrare né dare una battaglia finale. In primis i nuovi diritti e doveri - sempre considerando che, se c'è un diritto, qualcuno è obbligato a fare qualcosa, altrimenti si tratta di una mera dichiarazione. Ma i nuovi diritti nascono così: all'inizio sono dichiarazioni; nella prassi poi vanno trovando le proprietà specifiche che le conflittive ontologie giuridiche vanno consentendo. Il tema è di primaria importanza per il numero delle persone coinvolte e per la cogenza che queste esigono come condizione dell'espansione della rete.

INTERNET HA UN SUPPORTO TOTALMENTE MATERIALE

Poi un tema che per i giuristi è stato fin ora letale: tutto Internet, dai "dischi rigidi" (hard disk) dove risiede il messaggio, ai mezzi più svariati di trasmissione fino agli host e poi agli strumenti per la derivazione ad un utente, è tutto maledettamente materiale. È materiale l'orientamento dei nuclei di

ferrite che costituiscono il documento nel "disco rigido" della macchina, è materiale la conformazione in pacchetti di trasmissione, è materiale la trasmissione, è materiale il luogo del host, è materiale l'indirizzo del ricevente. Materiale vuol dire che ha una corposità nel tempo e nello spazio, che può viaggiare, ma anche in un mezzo materiale che è l'energia. Per molti addetti ai lavori queste sono ovvietà.

Non lo sono nel mondo giuridico dove si pensa, si ipotizza, una sorta di immaterialità intrinseca al digitale, il che comporta nelle ontologie giuridiche delle cantonate straordinarie. Essendo materiali i documenti elettronici rientrano nella definizione di documento di Carnelutti [6] e possono essere danneggiati, sottratti, rubati, etc. E hanno bisogno di un luogo fisico di riferimento: se si ha una pagina web si deve avere un dominio. Questo comporta problemi molto seri di controllo e sicurezza da una parte, di rispetto della privacy dall'altra.

Una parte importante di questo Quaderno si occupa di quanta sicurezza rispettando quanta riservatezza [7]. Occupandoci dei diritti non possiamo ignorare il fatto che per una grande parte dell'umanità l'accesso a Internet non si pone nemmeno come diritto, dato che non si pone dal punto di vista fattivo: non hanno reti, non hanno computer. In casi di estrema povertà il famoso diritto del consumatore diventa un diritto al consumo, seppure non esista ancora una letteratura consistente sul tema. Una osservazione aggiuntiva: alcuni diritti, come quello al consumo, attraversano tutte le discipline giuridiche dal diritto privato all'amministrativo dimostrando che il mutamento sociale produce profondi cambiamenti nelle discipline sociali che lo regolano.

Una considerazione elementare consiste nel fatto che ogni invenzione umana importante è al contempo pericolosa. Quasi si potesse dire che l'importanza di una scoperta scientifica è misurabile in termini della sua pericolosità. La più grande scoperta del secolo scorso - la fusione atomica - è allo stesso tempo la più pericolosa. Internet non può evadere da questa logica. Internet è pericolosa e, attraverso Internet, si possono commettere dei danni a cose e persone (delitti) dei quali abbiamo solo un panorama incompleto.

INTERNET FUNZIONA ANCHE GRAZIE ALLA SOLIDARIETÀ E LA COLLABORAZIONE

Ma non tutti sono problemi. Come nella vita, in Internet c'è la spietata competizione che comporta un occhio vigile verso gli abusi, ma anche una cooperazione che rende molti traguardi possibili grazie all'aiuto di molti e di tecniche di lavoro non conflittuali dove il profitto di uno non è necessariamente la perdita di un altro ma il guadagno (non necessariamente paritetico) di tutti.

La cooperazione in forum di discussione e gruppi di lavoro comuni sono un mezzo importante per raggiungere traguardi dei quali beneficiano tutti. Internet è una parte della vita moderna, quindi con le sue caratteristiche di lotta tra la regolazione e la forza.

La posizione aristotelica dell'orror vacui è stata sconfessata con la spiegazione di Torricelli sulla pressione atmosferica ma, nel mondo politico e giuridico, forse possiamo dire che c'è un orror vacui: quando il privato si può fare uno spazio, dentro, accanto o contra legem, se lo fa. Poi il problema è ristabilire gli equilibri, il che risulta difficile.

Il tema dell'assegnazione dei domini sembra un fatto meramente di catalogo, ma nasconde molto di più: battaglie spietate per una sigla come per esempio "ue" che l'America latina, dove si terrà il prossimo Internet Governance Forum, non è mai riuscita ad ottenere. La risoluzione per pochi voti contraria alla sigla "xxx" e le beghe che ci sono in questo momento in Cile perché un signore, Andrés Chapero, ha ottenuto il sito youtube.cl, contestato oggi dalla importante impresa americana, YouTube.

NOTE

[1] Vedi il paragrafo "La politica in Internet".

[2] Pare che Macchiavelli avesse usato la parola "governismo", ma è una citazione di seconda mano che faccio da una conferenza del Presidente della Regione Toscana, Martini, a Buenos Aires.

[3] Per il tema della democrazia diretta ci sarebbe molto da discutere: primo se è possibile, poi se è desiderabile, poi ancora come giocano la coppia "rappresentanza/partecipazione", vale a dire rappresentare chi? Partecipazione di quanti, e come?

[4] Posizione della sezione italiana di Internet society (ISOC Italia) in merito al filtraggio dei siti che offrono "gambling on line"

[5] Non staremo qui a discutere se c'è o non c'è la globalizzazione. Pensiamo che il solo fatto dell'esistenza di Internet mostra globalizzazione.

[6] "Cosa rappresentativa di una situazione giuridica"

[7] Le Patriot Act americane hanno mostrato fino a che punto il diritto dell'individuo può essere vanificato per un valore di scurezza nazionale, anche in un paese tradizionalmente liberale.

MANLIO CAMMARATA

Dal documento cartaceo al documento informatico: “dematerializzazione”?

Manlio Cammarata, nato a Trieste il 4 settembre 1947. Studi classici. Laureato in giurisprudenza nel 1971. Iscritto all'Albo dei giornalisti dal 1973. Esperto dei problemi dell'informazione. Oltre all'attività giornalistica, lavora come consulente in diritto dell'informazione e delle nuove tecnologie. Fondatore e direttore, dal 1997, della rivista telematica InterLex (www.interlex.it), il primo periodico telematico italiano sul diritto delle tecnologie.

Dalla carta al bit, dal "faldone" alla memoria elettronica. Da più di vent'anni è in corso un cambiamento sostanziale nella gestione delle pratiche amministrative, sia nel pubblico sia nel privato. I vantaggi dell'informatizzazione sono così noti che non è il caso di elencarli ancora una volta, così come sono noti i problemi. Questi possono essere divisi in due ordini.

Il primo è dato dall'imposizione di un cambiamento culturale profondo in tempi troppo brevi. Processi e conoscenze sedimentati da secoli devono essere sostituiti da nuovi processi e nuove conoscenze nell'arco della vita lavorativa di una persona, mentre prima il cambiamento richiedeva diverse generazioni. Ed è un cambiamento inarrestabile e irreversibile.

Il secondo ordine di problemi riguarda la normativa. Priva di un retroterra consolidato, in continuo assestamento, con in più le difficoltà di comprensione reciproca tra giuristi e tecnologi. Molti uomini di legge non riescono o non vogliono acquisire le indispensabili conoscenze tecniche di base, mentre chi lavora con le tecnologie spesso considera il diritto come un'inutile sovrastruttura, che complica il lavoro. In effetti, se si considera il complesso normativo disegnato dalla confusa direttiva 1999/93/CE e dalle sue ripetute e ancor più confuse attuazioni nell'ordinamento italiano, ci si rende conto che il problema di assumere le conquiste della tecnologia nell'ordinamento giuridico è ben lontano dall'essere risolto.

Tuttavia il progresso non può non innescare una vera e propria "rivoluzione culturale", che comporta la sostituzione dei processi basati sui documenti cartacei con processi basati su documenti in formato digitale e sulla loro gestione con strumenti informatici e telematici. Ma il passaggio "dalla carta al bit" è traumatico. I documenti di carta hanno una consistenza fisica evidente: si vedono, si toccano, si custodiscono in luoghi determinati nei quali l'uomo può andarli a cercare e prelevare. I secondi no: sono "da qualche parte" in un sistema informatico, per vederli e trattarli

occorre una macchina, a volte appaiono inaspettatamente diversi dalla loro precedente epifania, a volte scompaiono o sembrano scomparsi.

Occorrono competenze nuove. E tutto questo provoca un comprensibile disagio in chi è da sempre abituato a lavorare con i documenti di carta, i "faldoni", i grandi archivi. È però un fatto che lo sviluppo dell'e-commerce, dell'e-government e di qualsiasi altra attività con sistemi informatici implica necessariamente la sostituzione dei documenti cartacei con documenti in formato digitale, cioè composti da sequenze di bit. Questo processo è generalmente descritto come "dematerializzazione" dei documenti, perché al posto della carta ci sono i "bit", unità di misura che vengono di volta in volta rappresentate da variazioni di tensione elettrica, di carica magnetica, di riflessione ottica eccetera. Qualcuno osserva che il termine "dematerializzazione" non è corretto, perché anche nel documento digitale esiste sempre qualcosa di "materiale", che in ultima analisi è uno stato fisico della materia (elettrico, elettronico, magnetico, ottico…).

Questo è vero, ma i problemi sono altri. Cerchiamo di metterli a fuoco per capire se è opportuno parlare di "dematerializzazione" dei documenti nell'applicazione delle tecnologie al mondo del diritto.

IL DOCUMENTO E LA SUA VALIDAZIONE

Sappiamo tutti che cosa è un documento cartaceo e quali possono essere, di volta in volta, i suoi effetti giuridici. Invece non sempre abbiamo le idee chiare su che cosa sia un documento informatico e questo comporta non poche incertezze sui suoi effetti giuridici. Siamo certi solo che non è una "cosa", che possiamo toccare, vedere, verificare. Sapere che esso è fisicamente presente da qualche parte, sotto forma di bit, non ci aiuta. Non possiamo prendere in mano i bit, guardarli, capire che cosa significano. Per di più sappiamo che sono "volatili", che possono sparire, o che la loro sequenza può cambiare senza lasciare traccia del cambiamento. Fra l'altro questo significa che i bit, di per sé, non possono offrire alcuna certezza legale. Il problema della "certezza" dei bit, come ormai tutti sanno, si risolve con le "segnature digitali" (o "elettroniche" - electronic signatures nella direttiva 1999/93/CE), fra le quali si annovera la "firma digitale" (o "elettronica " [1]).

Si tratta di procedure informatiche, basate su complessi calcoli matematici, che operano una crittografia irreversibile su un riassunto del documento (hash). La segnatura assume il valore giuridico di una firma autografa quando è generata con determinate procedure di sicurezza, mentre la titolarità della chiave segreta di cifratura è attestata da un soggetto qualificato.

La segnatura digitale "congela" il contenuto del documento informatico, non perché lo renda sostanzialmente immodificabile, ma perché consente di verificare se ci sono state alterazioni dopo la generazione della segnatura stessa. Inoltre dà la possibilità di attestare legalmente l'attribuzione del documento stesso a un determinato soggetto, nel caso di una segnatura con valore di firma. In questo modo il documento informatico può avere, nella maggior parte dei casi, gli stessi effetti giuridici del documento cartaceo.

Ma c'è una differenza sostanziale tra la validazione [2] del documento cartaceo e quella del documento informatico. Nel primo i segni di validazione (firme, timbri, filigrane…) sono impresse sul supporto stesso, sicché contenuto, segni di validazione e supporto formano un corpo unico e inscindibile. La copia del documento cartaceo, come sappiamo, è per l'appunto "copia" e non un altro originale con gli stessi effetti.

Invece la validazione di un documento fatto di bit è composta da segnature fatte a loro volta di bit, sicché è possibile trasferire o duplicare un documento informatico insieme alle segnature che lo validano. Il documento può risiedere nella memoria volatile di un computer (e allora sarà rappresentato da grandezze elettroniche), in un disco magnetico (i bit saranno costituiti da cariche magnetiche), in un disco ottico (variazioni fisiche di una superficie che riflette la luce). I bit potranno essere trasferiti su un cavo metallico (variazioni elettriche) o ottico (variazioni luminose) e via elencando. In tutti questi differenti stati fisici il documento informatico mantiene i suoi effetti giuridici se insieme al contenuto sono presenti anche le segnature [3].

Possiamo quindi dire che lo stato fisico in cui di volta in volta si può trovare un documento informatico, ovvero la materia che lo rappresenta è del tutto indifferente per i suoi effetti giuridici.

Si vede qui la fondamentale differenza ontologica tra la validazione del documento tradizionale e quella del documento informatico: la prima è inscindibilmente legata al supporto materiale, tanto che cambiando il supporto occorre una nuova validazione; la seconda è legata al contenuto, tanto che il documento può essere trasferito da un supporto all'altro, duplicato o trasmesso a distanza, senza perdere i suoi effetti giuridici.

Dunque il supporto materiale è solo un "accidente" del documento informatico e il questo senso va intesa la qualificazione del documento informatico come "documento immateriale". In altri termini,

il documento informatico è un documento la cui espressione materiale (continuamente variabile) non ha (o può non avere) alcun effetto sul piano giuridico.

LA "FISICITÀ" DEL DOCUMENTO INFORMATICO

Possiamo anche considerare il problema da un altro punto di vista. È infatti possibile immaginare i bit come "segni" presenti su certi supporti e quindi paragonarli a segni impressi sulla carta o su qualsiasi altro supporto fisico. Ma scopriamo subito una differenza fondamentale: nessun essere umano è in grado di comprendere il contenuto di un insieme di bit senza l'intermediazione di una macchina, che elabori i segni digitali trasformandoli in segni leggibili. Inoltre il documento cartaceo può essere preso in mano, consegnato o inviato fisicamente a un altro soggetto, può essere letto direttamente da una persona.

La sua distruzione in molti casi determina l'annullamento dei suoi effetti giuridici, anche se ne esiste una copia. Il documento cartaceo è una cosa concreta percepibile dai nostri sensi, il bit è una astrazione. Per inquadrare meglio il concetto possiamo fare l'esempio dell'assegno bancario: solo la presentazione dell'originale obbliga l'istituto di credito al pagamento; una copia, anche autenticata, non può avere lo stesso effetto. Lo stesso discorso vale per la cambiale, la procura speciale e altri documenti dei quali una norma imponga l'esibizione o la consegna dell'originale. La copia, quando è ammessa, non è l'originale e può avere effetti giuridici diversi. Inoltre deve essere in qualche modo validata come rispondente all'originale, attraverso un'autenticazione o anche solo un'autocertificazione.

La natura materiale del documento cartaceo è quindi essenziale per i suoi effetti giuridici. Invece il documento informatico non si tocca, non si legge direttamente (occorre una macchina per tradurre i bit in segni leggibili) può presentarsi in modi diversi, può essere duplicato un numero infinito di volte. La sua esistenza fisica sfugge ai nostri sensi: quello che vediamo sullo schermo del computer non è "il" documento, ma una sua rappresentazione. Noi possiamo prendere il mano un documento di carta e sapere che documento è. Ma se prendiamo un disco ottico, sappiamo solo che "può" contenere uno o più documenti: nella sua essenza materiale non ci dice nulla di ciò che effettivamente contiene. Le migliaia di documenti che possono essere archiviati in un disco ottico non hanno alcuna evidenza fisica che possa essere percepita attraverso i nostri sensi.

Nel documento tradizionale il contenuto è inscindibilmente legato al supporto. La natura del contenuto e di eventuali segnature presenti sul supporto determinano il tipo o il grado di effetti

giuridici propri del documento. In ogni caso l'integrità di un documento tradizionale è quasi sempre verificabile attraverso la verifica dell'integrità del supporto materiale, dove per integrità intendiamo anche l'assenza di cancellature o sovrapposizioni di segni o la possibile falsificazione della firma o sottoscrizione. Invece per il documento informatico l'esame fisico non è possibile. Né la memoria temporanea di un computer né il supporto di memorizzazione né il mezzo trasmissivo (cavo o etere) possono in alcun modo rivelare, senza l'intermediazione della macchina il contenuto, l'integrità e la provenienza soggettiva di un documento.

Anche sotto questo punto di vista possiamo quindi concludere che la "materia" costitutiva del documento informatico è indifferente ai fini dei suoi effetti giuridici e quindi che si tratta di un documento giuridicamente immateriale.

ALTRI ASPETTI DA CONSIDERARE

Ci troviamo dunque di fronte a una specie di immaterialità relativa. Vi sono infatti situazioni in cui l'esistenza fisica di un documento informatico può apparire rilevante. Un esempio si verifica quando un giudice ordina di sequestrare un file che risiede in un certo computer, o semplicemente di accertare quali file siano presenti in un certo computer.

Si deve però notare che queste operazioni in genere non coinvolgono gli eventuali effetti giuridici dei file in questione. Anzi, in molti casi non si tratta di documenti giuridici, ma di mere informazioni. Per esempio, un "log" non produce di per sé alcun effetto giuridicamente rilevante, ma può assumere (in presenza di determinate condizioni) il valore di prova in una causa. Si può anche acquisire un contratto di compravendita in formato digitale, sempre a fini di prova. Ma in ogni caso quel contratto, ove sia stato validamente formato, non produce effetti diversi se è presente in questo o quel server.

La collocazione fisica del supporto sul quale il documento informatico è presente può essere rilevante per altri motivi. Per esempio, può rilevare il fatto che una pagina internet che contiene informazioni diffamatorie risieda su un server posto in uno stato piuttosto che in un altro: si può porre sia un problema di giurisdizione sia un problema di perseguibilità del reato, nel caso in cui i suoi effetti si verifichino in uno stato diverso da quello di provenienza del documento. Ma, a ben guardare, anche in questo caso non sono in gioco gli effetti propri del documento: un testo diffamatorio resta diffamatorio dovunque si trovi; il problema è la perseguibilità dell'eventuale reato.

Altri problemi collegati a quella che abbiamo definito come immaterialità relativa del documento informatico sono legati alla sua archiviazione a fini storici. La scienza archivistica contempla i modi di conservazione non delle informazioni in sé, ma dei supporti, con le informazioni e le meta-informazioni che contengono. Quando il documento si presenta all'archivista sotto forma di bit, egli non trova tutti gli elementi che è abituato a classificare e conservare. Dispone infatti solo delle informazioni che sono oggetto del documento, delle eventuali segnature e dei dati relativi al processo elettronico che gli ha fornito il documento da archiviare. Che sono informazioni relative alla trasmissione del documento, non al documento stesso (a parte l'attestazione di integrità che si ottiene con la posta elettronica certificata). Ma si tratta, almeno in parte, di un falso problema: le informazioni che l'archivista non trova sono quelle normalmente legate al supporto. Che, come abbiamo visto, non è rilevante per gli effetti del documento.

Passando il documento sul supporto di archiviazione, l'archivista non altera in alcun modo il contenuto del documento, ma solo, eventualmente, la sua rappresentazione.

CONCLUSIONE

La questione prospettata in questo brevissimo studio può sembrare secondaria, un caso di lana caprina o una mera disquisizione terminologica. Invece è un problema importante sotto diversi aspetti. Infatti il documento informatico impone in primo luogo di adottare per la sua gestione procedure del tutto diverse da quelle tradizionali, perché ogni volta che è destinato a produrre effetti giuridicamente rilevanti è necessario verificarne la rispondenza ai requisiti richiesti per quei determinati effetti.

Occorrono quindi procedure informatiche (che possono essere molto più semplici e intuitive di quelle oggi in uso) per verificarne la validità e la provenienza, e quindi per la trasmissione, gestione e conservazione. Fra l'altro, la verifica del documento informatico offre (in linea di principio) certezze più forti del controllo "a occhio" dei timbri e delle firme su un foglio di carta. Considerare il documento informatico come non materiale aiuta la comprensione dei problemi e facilita il passaggio alla gestione informatica.

Sul piano processuale il documento informatico richiede particolari cautele nelle fasi di esibizione e nell'eventuale giudizio di verificazione o nella querela di falso, perché allo stato attuale non è immaginabile che si possano avere processi civili diversi quando i mezzi di prova sono cartacei o

informatici. L'equiparazione dei documenti informatici a quelli cartacei è un passaggio essenziale, che era stato risolto con il DPR n. 513 del 1997, ma che si è poi dissolto nelle sconsiderate modifiche normative che sono seguite (peraltro di dubbia costituzionalità).

La considerazione, teoricamente corretta, che la falsificazione di un documento informatico è molto più difficile di quella di un documento di carta, non può portare alla conclusione che il primo è "più sicuro" del secondo. Una certezza di più alto livello si potrà avere solo quando nella generazione della firma digitale sarà possibile usare un segno biometrico [4].

Fino a quel momento potremo avere una fortissima certezza materiale e legale dell'integrità del documento, dovuta ai calcoli matematici posti a fondamento della segnatura digitale. Invece la certezza legale dell'attribuzione del documento a un determinato soggetto è legata alla presunzione del possesso, nelle mani dello stesso soggetto, del "dispositivo di firma" e del fatto che lui solo è a conoscenza del codice segreto che attiva la procedura. Con le attuali norme italiane questa presunzione è molto debole. È infatti noto che moltissimi dispositivi di firma, con il relativo codice segreto, non vengono consegnati ai legittimi titolari, ma a intermediari.

Può sembrare paradossale che il valore effettivo di un documento essenzialmente non materiale derivi da un atto assolutamente materiale, come la consegna di un oggetto fisico nelle mani di una persona fisica, che dovrebbe essere stata preventivamente identificata con certezza, come prevedevano le norme del 1997. Insomma, la dematerializzazione può essere un concetto utile, ma deve essere "maneggiato" con i piedi ben piantati per terra...

NOTE

[1] Poiché i bit si possono “materializzare” in diversi stati, sarebbe opportuno non usare l’aggettivo “elettronico” ogni volta che si parla di oggetti informatici. A seconda del supporto su cui sono registrati, i bit possono essere elettronici, ottici, magnetici. Al limite si potrebbero rappresentare con pioli di legno. Il termine corretto, in particolare per le segnature e le firme, è “digitale”.

[2] La normativa sui documenti informatici usa il termine “autenticazione”, come pedissequa traduzione dell’inglese authentication. Ma nel nostro ordinamento l’autenticazione è un istituto particolare, definito dell’art. 2703 c.c.

[3] Per questo motivo del documento informatico possono esistere n esemplari identici, e quindi con gli stessi effetti giuridici. Si parla quindi di “duplicati” e non di “copie”.

[4] Nella generazione della firma digitale, il dato biometrico deve essere impiegato per l’attivazione della procedura di sottoscrizione, non come chiave di cifratura, per motivi di sicurezza. La tecnologia è pronta da tempo, ma la sua utilizzazione presenta ancora problemi che ne impediscono l’impiego su vasta scala.

BAN KI-MOON

Messaggio di invito al Meeting Igf di Rio
del Segretario Generale delle Nazioni Unite

The inaugural Internet Governance Forum meeting in Athens, Greece, proved a great success. This year, the Government of Brazil has generously offered to host the second IGF meeting in Rio de Janeiro from 12 to 15 November 2007. I take this opportunity to accept the Government's offer, and to invite all stakeholders to attend this important gathering. The meeting will be open to all World Summit on the Information Society accredited entities. Other institutions and persons with proven expertise and experience in matters related to Internet governance may also apply to attend.

A broad-based consultative process led by my Special Adviser for Internet Governance, Mr. Nitin Desai, has laid the groundwork for another successful Forum. This process included preparatory meetings open to all stakeholders held in Geneva in February and May this year. These consultations produced general agreement that the second Forum should build on the success of Athens, and retain its overall theme of "Internet Governance for Development", with capacity-building remaining a cross-cutting priority.

There was also broad support for retaining the four main themes of the inaugural meeting: access, diversity, openness and security. In addition, a fifth theme, "critical Internet resources", will also be added to the agenda, together with consideration of emerging issues. The process leading to the Rio de Janeiro Forum is an integral part of the meeting itself. That is why I also encourage all stakeholders to engage in the online discussions hosted by the IGF secretariat on its website.

These interactive forums help guide the preparations of the Rio de Janeiro meeting, and provide substantive input for the various items on the agenda.

The Forum is modest in its means but not in its aspirations. Its hallmark is multi-stakeholder collaboration, based on the exchange of information and the sharing of best practices. This new form of international cooperation is both inclusive and egalitarian. And it presents governments, the private sector and civil society, including academic and technical communities, with the opportunity to work together towards a sustainable, robust, secure and stable Internet, as envisioned by the Tunis Agenda for the Information Society.

In that spirit, I hope you will all be able to join us in Rio this November.

FRANCESCO CELENTANO, GERARDO A. CAVALIERE, MICHELE IASELLI, DAVIDE MERLITTI

Spamming e furti di identità

Francesco Celentano, Avvocato,Titolare della cattedra di Informatica, Università Giustino Fortunato di Benevento. Cultore della materia di Informatica, Università degli Studi di Foggia. Riveste numerosi incarichi per l'Avvocatura in materia di Informatica in ambito ordinistico, regionale ed europeo. È proprietario ed editore della testata giornalistica online Studio Celentano.

Gerardo A. Cavaliere, Avvocato, Dottore di ricerca in Bioetica e sistemi giuridici, Università degli Studi di Foggia. Cultore della materia di Informatica, Università Giustino Fortunato di Benevento. Giornalista pubblicista, scrive sulla testata giornalistica Studio Celentano.

Michele Iaselli, Avvocato, Docente di Legislazione new economy, Università degli Studi di Ferrara. Funzionario del Ministero della Difesa. Autore di decine di monografie, scrive sulla testata giornalistica Studio Celentano.

Davide Merlitti, Consulente informatico, Scuola Normale Superiore di Pisa. Scrive sulla testata giornalistica Studio Celentano.

Celentano, Cavaliere, Iaselli e Merlitti insieme hanno pubblicato, da ultimo: Manuale breve di informatica per avvocati, Utet, 2007.

DEFINIZIONE DI SPAMMING COME ABUSO DI POSTA ELETTRONICA

Uno dei temi più importanti e discussi in Rete è il fenomeno dello spamming. Qualunque utente di Internet, ormai, conosce questa piaga, che accomuna democraticamente i navigatori di tutti gli Stati del mondo. Eppure questo fenomeno di enorme e attuale rilevanza a livello mondiale coinvolge uno degli strumenti di Internet più "antichi": la posta elettronica.

Essa è definita come quel sistema informatico che permette una comunicazione asincrona uno-a-uno o uno-a-molti. Per comunicazione asincrona si intende quel servizio che non richiede l'interattività simultanea fra i processi coinvolti su host della Rete (posta elettronica, Www, Ftp), mentre per comunicazione sincrona si fa generalmente riferimento a quei servizi che richiedono l'interattività fra tali processi.

Per molti la posta elettronica, electronic mail (abbreviato in e-mail), rappresenta la più frequente ed efficace forma di comunicazione post-moderna. Nata come mezzo di comunicazione essenziale

subito dopo la nascita di Arpanet [1], la posta elettronica è stata costantemente migliorata al punto da raggiungere oggi un elevatissimo grado di innovazione tecnologica.

I primordi della posta elettronica possono essere ricercati fin negli anni Sessanta, allorquando iniziarono a essere commercializzati i primi computer che potevano eseguire più applicazioni contemporaneamente. A quel tempo vennero scritti alcuni programmi che consentivano lo scambio di messaggi testuali fra computer, ma unicamente all'interno dello stesso gruppo di utenti che condividevano un computer. Fu proprio in quegli anni che si scelse il carattere "@" come elemento che poteva caratterizzare gli indirizzi e-mail rispetto ad altri indirizzi relativi al mondo di Internet.

Alla fine del 1971 Ray Tomlinson sviluppò la prima applicazione per lo scambio di e-mail all'interno di Arpanet: si chiamava Cpynet ed era un software capace di copiare file sulla Rete e di informare i colleghi, inviando loro una e-mail con le istruzioni per usare il nuovo programma. Fu Tomlinson a scegliere la "chiocciola" come simbolo standard per indicare un indirizzo di posta elettronica [2].

Spam, nel vocabolario inglese, indica la "carne di maiale in scatola" ed è il risultato della contrazione fra le parole spiced e ham. La parola spam, però, attualmente non è utilizzata per indicare scatolette di carne e simili, quanto piuttosto un fastidioso e non richiesto invio di messaggi pubblicitari nella nostra cassetta elettronica delle lettere (vietato dall'art. 8 della Netiquette, in cui si proibisce l'invio "tramite posta elettronica di messaggi pubblicitari o comunicazioni che non siano stati sollecitati in modo esplicito" [3]) .

Il nesso fra le parole spam e l'appena citato invio non desiderato di posta deriva da una scenetta comparsa in un episodio della serie televisiva Monty Python's Flying Circus. Una coppia entra in un ristorante per ordinare da mangiare. La cameriera si avvicina, ma non riesce a prendere le ordinazioni. Un gruppo di gioviali avventori, infatti, - con dei simpatici elmi in testa (a mo' di vichingo) - disturba il silenzio del locale con una canzone che fa "Spam, spam, spam…" e che impedisce ai tre soggetti di comunicare fra loro. Alla fine, il marito è costretto a ordinare nient'altro che dello spam! I messaggi di spamming sono suddivisi in diverse tipologie.

Per quanto concerne il tipo di destinatario che le riceve vi sono: i messaggi inviati a decine di newsgroup (in questo modo sono colpiti tutto gli iscritti al newsgroup); e quelli inviati a un singolo utente ben individuato. Riguardo al contenuto, invece, i messaggi di spam possono essere

classificati in tre tipologie: Hoax (cioè le c.d. catene di S. Antonio); e-mail inviate da virus; Unsolicited Commercial E-mail (Uce). In questa sede ci si occupa dell'ultima categoria elencata, le Uce.

I soggetti (c.d. "spammers", o "spammatori") che svolgono questo tipo di attività a danno di tutti gli utenti riescono a ottenere gli indirizzi di posta mediante l'uso di software specifici. Questi programmi scandagliano la Rete intera (e, quindi, anche le pagine web più nascoste e ramificate, e non solo le home page) e ogni volta che individuano un indirizzo così composto: tuonome@dominio.it (per esempio) lo memorizzano. Una volta individuato e registrato, l'indirizzo viene inserito nel campo dei destinatari cui saranno dirette le e-mail. Pur trattandosi di un fenomeno meramente pubblicitario, esso, per le modalità con cui è organizzato e gestito, lede gli interessi di tutti quei navigatori cui corrispondono gli indirizzi di posta.

L'utente, dunque, pur non avendo acconsentito all'invio dei messaggi incriminati non può fare altro che restare inerte o utilizzare uno dei tanti rimedi oggi esistenti per combattere la "lotta" contro lo spamming.

CARATTERISTICHE DELLO SPAMMING

Secondo la Organisation for Economic Co-operation and Development [4] vi sono alcune peculiarità che contraddistinguono lo spam. Fra loro possono essere suddivise in due tipologie: quelle di primaria importanza e quelle secondarie.

Fra le prime troviamo:

- messaggio elettronico: i messaggi di spamming sono inviati elettronicamente. Mentre la e-mail è lo strumento più utilizzato come canale di invio, altri circuiti possono essere la messaggistica immediata (IM) e i brevi messaggi di testo via telefono cellulare (Sms);
- inviate in blocco (bulk): i messaggi sono tipicamente inviati in massa, ma possono essere spediti in piccoli gruppi di lettere da account di posta elettronica gratuiti;"
- non richiesto: lo spam è inviato senza il consenso o la richiesta da parte del destinatario. È difficile, comunque, distinguere a volte lo spamming da contatti per i quali esiste effettivamente un determinato rapporto fra destinatario e mittente;
- commerciale: di solito lo spam ha uno scopo pubblicitario: la promozione o la vendita di determinati prodotti o servizi. Tuttavia, alcuni messaggi non commerciali possono essere

considerati altri esempi di spam, per esempio, quelle lettere dal contenuto politico o recanti virus.

Fra le secondarie:

- utilizzo di indirizzi collezionati senza previo consenso: gli spammers usano spesso indirizzi e-mail che sono stati raccolti senza il consenso esplicito del legittimo proprietario;
- non volute: nessuno ha mai richiesto determinati messaggi;
- ripetitive: molto spesso gli spammers inviano più volte gli stessi messaggi ai medesimi destinatari;
- indiscriminato: tipicamente lo spam è inviato in una maniera indiscriminata, senza cognizione di quello che può essere l'impatto che si avrà sul destinatario finale; "
- inarrestabile: è quasi impossibile essere immuni dal ricevere messaggi, seppure non desiderati;
- anonimo o camuffato: i messaggi di spam sono spesso trasmessi con artifici tecnici mediante i quali viene nascosta o camuffata una serie di informazioni, che afferiscono al mittente (header del messaggio);
- contenuto illegale, offensivo, fraudolento o ingannevole: il contenuto dei messaggi può essere di vario genere e può anche essere contrario alle leggi in vigore nel Paese di residenza del destinatario.

IL REPERIMENTO DEGLI INDIRIZZI

Prima di organizzare l'attività, gli spammers devono ovviamente detenere un certo quantitativo di indirizzi di posta elettronica, cui inviare i messaggi. È opportuno, allora, procedere a una necessaria (e quanto mai ampia) raccolta dei dati, oggetto della propria "occupazione". Affinché gli attacchi riscuotano un discreto successo, infatti, i messaggi non sollecitati devono essere inviati al maggior numero di indirizzi di posta. Questa fase, dunque, appare fondamentale e prodromica alla vera e propria attività di spamming e deve essere gestita in maniera alquanto accurata.

È necessario cercare di coniugare, infatti, due criteri precisi: velocità di reperimento degli indirizzi e grande quantità dei medesimi. La realizzazione di sistemi di spamming (attraverso programmi di spamming, c.d. spamware) è - pur sempre - una specie di attività commerciale. Perciò si deve cercare di raggiungere il potenziale cliente nel più breve tempo possibile.

Una prima tecnica di reperimento degli indirizzi e-mail consiste nell'"inventarli". Gli spammers, infatti, sanno quali sono i mail server più famosi e popolari in Rete e sono a conoscenza, quindi, del fatto che ogni mail server ospiterà le caselle di posta di svariati utenti. La maggior parte dei navigatori creano il proprio account di posta elettronica di solito indicando il proprio nome. Per esempio, negli Usa, ci saranno centinaia di migliaia di John, Mike, Paul, ecc. In Italia altrettanti Giovanni, Michele, Paolo, ecc. L'attività degli spammers è quella di postulare l'esistenza di svariati account di posta, partendo da prestabiliti provider che forniscono servizi di posta elettronica. Tale lavoro, però, non dà sempre buoni risultati. Innanzitutto molti utenti utilizzano nickname, poi taluni usano anche segni di interpunzione nel proprio nome utente, talaltri, invece, includono nel proprio ID anche dei numeri, ecc.

Per questo motivo, è fondamentale l'utilizzo dei c.d. "generatori random". Si tratta di software - chiamati anche dictionary attack - che permettono di generare automaticamente un numero infinito (almeno in teoria) di indirizzi di posta elettronica, afferenti a uno specifico dominio. Poniamo il caso del dominio @tin.it: il programma invierà il messaggio in primis all'indirizzo a@tin.it, poi aa@tin.it, poi b@tin.it, ecc. Poiché si presume che nella realtà non vi siano così tanti indirizzi nelle modalità e nelle quantità "pensate" da uno di questi generatori random, moltissime e-mail torneranno indietro, per inesistenza del destinatario.

Lo spammer, invece, che vuole andare "a colpo sicuro" dovrà optare per altri strumenti e andare alla ricerca di "veri" indirizzi di posta. Una seconda tecnica, dunque, consiste nell'utilizzo dei c.d. strumenti di "traino", ossia di aspirazione di indirizzi. Poiché, solitamente, gli indirizzi e-mail sono tenuti privati (e sono lasciati a poche persone) lo spammer non potrà entrarvi in possesso, ma - come detto supra - potrà solo postularne l'esistenza. Allora è d'obbligo spostarsi in ambiti in cui è più facile che si trovino indirizzi e-mail lasciati "in pubblico dominio": il web, i forum e i newsgroup. In questa attività, lo spammer si avvale di specifici software, che esplorano automaticamente le pagine web, i forum e i newsgroup alla ricerca di caratteri disposti in maniera tale che sembrino degli indirizzi e-mail.

Questi programmi - chiamati spambots - hanno la capacità anche di entrare nei codici Html di una pagina web e leggere gli indirizzi di posta ivi contenuti (quindi, non solo se la e-mail è indicata "in chiaro" nella pagine web). Essi, dunque, funzionano in base al principio di una navigazione automatizzata su siti web e sugli spazi pubblici di Usenet utilizzando o un elenco di Url specificati preventivamente o parole chiave sottoposte a motori di ricerca, che permettono di costituire un

elenco di Url pertinenti. Il software effettua quindi una raccolta sistematica di tutti gli indirizzi e-mail trovati sulle pagine di questi siti o nei forum.

Gli spammers, però, utilizzano anche altri sistemi che in maniera più subdola reperiscono gli stessi dati, e ciò non tanto per l'uso di un software, ma grazie allo stesso ignaro navigatore. Essi possono creare, per esempio, dei siti web (solitamente dal contenuto erotico, per attirare un maggior pubblico) all'interno dei quali vengono richiesti alcuni dati per l'accesso al servizio. Oppure si possono realizzare siti web che, con lo stesso meccanismo appena indicato, una volta richiamato l'utente, "rubano" alcune informazioni personali dal nostro browser (e, quindi, per esempio, il nostro indirizzo e-mail). Un altro modo, piuttosto originale, per racimolare indirizzi di posta è quello realizzato da alcuni siti che offrono la possibilità di inviare "messaggi anonimi".

Per capire meglio di cosa si tratta, si può schematicamente riassumere il procedimento in questi termini. Il sito "A" offre a un altro (sito "B") la possibilità di inserire nella home page di quest'ultimo un piccolo form Html, nel quale l'utente potrà usufruire di un servizio di messaggistica anonima, fornito dal sito A. Come si evince dalla terminologia utilizzata, il surfer farà pervenire a un altro navigatore un messaggio anonimo.

Fin qui tutto semplice. Il problema giuridico (ma anche etico da certi punti di vista) si realizza successivamente. Il destinatario del messaggio riceverà, attraverso i server del sito A, una notifica di ricezione e, all'interno di questa, potrebbero essere contenute varie informazioni pubblicitarie, oltre al messaggio anonimo inviatogli. Questa procedura consente a un qualsiasi navigatore di inviare messaggi anonimi (pratica lecita, perché rientrante nel più generale diritto all'anonimato dell'individuo), ma attraverso un sistema che lo inganna, poiché è finalizzato molto probabilmente alla raccolta del suo indirizzo di posta e di quello dei destinatari, per finalità che è difficile non scorgere nella generazione di spam [5].

INVIO DEI MESSAGGI

Una volta reperiti tutti gli indirizzi che sembrano sufficienti, gli spammers iniziano la vera fase di invio. A tal fine essi possono utilizzare anche normalissimi programmi per la gestione della posta elettronica. Nella maggioranza dei casi essi nascondono gli header (cioè quei dati informativi iniziali) della lettera per rendere più difficoltosa la ricostruzione del percorso di quella determinata e-mail.

Siamo, dunque, nella c.d. fase "di spinta", ossia dell'invio massiccio di e-mail. Gli strumenti c.d. "di spinta" sono motori che permettono di realizzare gli invii in massa senza passare da un server di posta elettronica specifico o di un certo Isp. I prodotti che si trovano attualmente sul mercato permettono all'elaboratore su cui sono installati di comportarsi come un vero e proprio server di posta elettronica, senza correre il rischio di dover essere vincolati a degli Isp, che potrebbero contestare la saturazione di banda.

Questi motori sono in grado di superare i filtri anti-spam dei server di posta elettronica e permettere una perfetta falsificazione delle intestazioni di messaggio. È abbastanza paradossale che si possano trovare apertamente sul mercato tali prodotti, commercializzati da distributori apparentemente ufficiali, sapendo che una parte delle loro funzionalità corrisponde a modalità di intasameto del traffico su Internet

LA VENDITA DEGLI INDIRIZZI

È opportuno notare, inoltre, che non sono rari i casi in cui i dati faticosamente raccolti vengano riuniti in "pacchetti" per la vendita ad altri spammers. I tagli e i prezzi variano a seconda del caso specifico, ma sta di fatto che i nostri indirizzi divengono merce di scambio di grande valore. L'offerta di servizi si presenta schematicamente in due grandi categorie di prestazioni: l'organizzazione di campagne (host-spamming) e l'intermediazione di file d'indirizzi e-mail.

Nel primo caso viene offerta una prestazione completa di servizi per l'organizzazione di campagne di spamming; varie piccole aziende ne fanno apertamente professione sulla Rete; le loro tariffe variano da 5 dollari al migliaio per una spedizione a 20 dollari al migliaio se il cliente vuole disporre degli indirizzi. Alcuni si sono specializzati nell'offrire un servizio "a prova di pallottola", ossia in grado di sfuggire in linea di principio alle azioni repressive degli Isp. I mediatori d'indirizzi sono abbastanza numerosi: varie società propongono offerte di membership comprendenti diverse formule d'abbonamento a elenchi d'indirizzi, ma che si sostanziano nella vendita di pacchetti di centinaia di migliaia di indirizzi.

Esistono anche offerte d'acquisto in linea di indirizzi immediatamente scaricabili. Gli elenchi mirati sono presentati per lo più in modo abbastanza vago; i criteri di selezione più comuni sono il paese, lo Stato, la città di residenza, il sesso, gli interessi, la professione e il settore d'attività. I centri d'interesse si scompongono in una cinquantina di segmenti correnti che ricordano la struttura dei grandi domini su Usenet.

METODI DI CONTRASTO ALLO SPAMMING

Senza scendere nel dettaglio dei numerosi metodi studiati per contrastare questo fenomeno [6], si ricorda che esistono fondamentalmente due categorie di anti-spam: quelle che si basano sul filtraggio della provenienza del messaggio e quelle che si basano, invece, sul filtraggio dei contenuti (euristico o bayesiano). Si può affermare che, fra tutte le tecniche elaborate, la più efficace è quella dell'analisi bayesiana del contenuto.

Tutti gli altri metodi sono falliti miseramente, a causa delle complesse difficoltà tecniche di bloccare in maniera del tutto sicura l'arrivo di messaggi spazzatura.

RASSEGNAZIONE DEGLI UTENTI

Il fenomeno dello spamming ha raggiunto ormai dimensioni elevate ed è in costante aumento. Al di là delle statistiche sulla sua diffusione [7], un dato è particolarmente significativo: oggi gli utenti (in particolare quelli statunitensi) si sono rassegnati allo spamming e lo vivono come un dato di fatto. È quanto emerge da una indagine svolta da Pew Internet and American Life Project, organizzazione attiva nello studio dell'impatto che Internet ha sulla società (famiglie, comunità, politica, ecc.).

EVOLUZIONE DEGLI ATTACCHI

Gli spammers, pur prediligendo la posta elettronica per consegnare i messaggi di advertising, hanno iniziato a usare anche altri canali. Il messaging spam, anche detto Spim (dalla contrazione delle parole spam e instant messenger), è quello spamming perpetrato tramite i sistemi di messaggistica istantanea, come Aol oppure Yahoo! Messenger.

Con l'esplosione dei blog, gli spammatori non si sono fatti sfuggire un nuovo strumento, per inserire messaggi pubblicitari in Rete. Gli spammers, dunque, si sono dedicati alla realizzazione di blog pieni di pubblicità e, per questo motivo, il nuovo fenomeno è stato chiamato Splog (dalla contrazione delle parole spam e blog). Un altro sistema recentemente diffusosi a macchia d'olio è quello dello spamming con immagini (c.d. image-spamming).

Gli spammers, infatti, per aggirare i filtri che analizzano le parole delle e-mail, inseriscono immagini che contengono ugualmente gli annunci pubblicitari, ma non vengono intrappolati nei filtri anti-spamming. L'uso di image-spamming è cresciuto notevolmente negli ultimi mesi, raggiungendo il 25% di tutta la pubblicità indesiderata che circola in Rete.

I PROBLEMI CAUSATI DALLO SPAMMING

Come è facilmente intuibile, il maggior problema che lo spamming crea (insieme a quello dei costi per ridurlo) è la rilevante ingerenza nella riservatezza personale degli utenti della Rete. Ogni navigatore sa che Internet è un mezzo utile per lo sviluppo, non solo del proprio business, ma anche della propria personalità. In quest'ultimo senso, l'utente della Rete è vagamente consapevole della sua possibilità di entrare nel mondo di altre persone, conoscendone le realtà seppure a migliaia di chilometri di distanza, e che ciò è direttamente proporzionale alle possibilità che altri entrino nel proprio mondo fatto di conoscenze, amicizie, lavoro.

Purtroppo, la maggior parte di questi "attentati" non è difficilmente conoscibile a un utente poco esperto della Rete. Vi sono infatti svariate modalità di interferire nella privacy di ognuno. Basti pensare solamente a tutti i cookies che si installano nel proprio computer a seguito della semplice visualizzazione di una pagina web o di un accesso alla posta elettronica e che permettono di reperire numerosi dati personali. Tali dati, se per un verso possono sembrare innocui, perché generati automaticamente dall'elaboratore, per l'altro possono essere visualizzati, copiati e diffusi da soggetti diversi senza che il legittimo proprietario sia consenziente.

Un recente modo per attentare alla riservatezza personale di ognuno è, senza ombra di dubbio, il fenomeno qui analizzato: lo spamming. Essere continuamente bersaglio della pubblicità via posta elettronica, infatti, non può che minare il fragile equilibrio, che la privacy personale cerca di mantenere in Rete. Si deve considerare, poi, che il proprio indirizzo di posta elettronica è custodito da soggetti che non sono stati autorizzati al relativo trattamento, ma che possono rivendere ad altri senza il nostro consenso.

Di questo passo quello che può essere un mezzo per intrattenere rapporti lavorativi e sociali - cioè l'indirizzo di posta elettronica - diventa oggetto nelle mani di terze persone, che non hanno altro scopo se non quello di sommergerci da messaggi indesiderati. Il piccolo spazio virtuale che ciascuno detiene nel "mare magnum" della Rete deve essere salvaguardato come lo spazio che "fisicamente" ognuno di noi possiede nella società. A tal riguardo oggi si parla proprio di una nuova forma di "entità individuale": la c.d. "electronic persona", ovvero, la "e-persona". Essa può essere definita come "quel vestito che ciascun navigatore indossa al momento del surfing e che può trasformare l'utente o in una entità diafana, capace di entrare in qualunque zona di Internet in

maniera anonima, oppure in un rigoroso e attento fruitore di contenuti accessibili nella Rete". Questa metafora sintetizza in poche parole la vera essenza dell'odierno navigatore in Rete.

Con pochi concetti si vengono a delineare le complesse sfere di diritti di cui ciascun utente dispone all'interno di Internet. Diritti che erano già riconosciuti dagli ordinamenti giuridici prima dell'avvento della Rete mondiale (come il diritto al nome, alla propria immagine, ecc.) e diritti che sono arrivati a compimento proprio in seguito alle particolari esigenze sorte con le nuove tecnologie (come il diritto alla privacy). Con il concetto di e-persona, dunque, si è voluta intravedere una sorta di "alter ego" della persona fisica umana.

La parte dell'uomo che entra in contatto (metafisicamente parlando) con gli strumenti della moderna tecnologia assume, di per sé, valore giuridico e merita rispetto per ciò che essa rappresenta: prolungamento ideale della persona fisica. La consapevolezza dell'esistenza di questa nuova dimensione dell'uomo rende opportuno un ulteriore passo.

Bisogna, infatti, riempire di contenuti giuridici questo alter ego. L'unico modo per compiere questo delicato "intervento" appare essere probabilmente quello di applicare anche a questa nuova dimensione i diritti personalissimi che spettano all'uomo in quanto persona fisica. Sono quei diritti che vengono "trovati" dal diritto oggettivo, poiché esistenti indipendentemente da ogni diritto oggettivo che li riconosca e che questo si limita a garantire. Sono i "diritti inviolabili dell'uomo", tutelati dalla nostra Costituzione all'art. 2 ("La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità").

Questo loro carattere di inviolabilità ha un duplice referente: sono diritti dell'uomo inviolabili da parte della pubblica autorità, nell'esercizio delle sue funzioni legislative, esecutive o giudiziarie; sono, inoltre, diritti dell'uomo inviolabili da parte degli altri uomini, nell'ambito dei rapporti fra privati. Hanno la peculiarità di essere protetti nei confronti di tutti i consociati (per cui rientrano fra i diritti assoluti), sono diritti che il loro titolare non può alienare né cui può rinunciare (diritti indisponibili). Sono diritti che non si prescrivono, che non si estinguono per il non uso prolungato nel tempo (diritti imprescrittibili).

Possono rientrare, pertanto, fra i diritti personalissimi della e-persona i seguenti diritti (elencati in maniera non esaustiva, poiché essi costituiscono una serie aperta).

a. Il diritto al nome, inteso sia come diritto all'uso del proprio nome (ossia come diritto a identificare se stessi con il proprio nome e come diritto di essere identificati dagli altri con esso) sia come diritto all'uso esclusivo del proprio nome. L'art. 9 codice civile tutela anche lo pseudonimo, solo nel caso in cui esso abbia acquistato l'importanza del nome e sino a quando tale circostanza sussista; importanza che si rapporta, come per il nome, in un determinato ambiente sociale (o ambito di socializzazione) e che svolge la medesima funzione identificativa e, al tempo stesso, differenziatrice di un soggetto e del suo proprio modo di essere (e di non essere) rispetto agli altri [8]. Quindi, appare plausibile conferire tutela giuridica anche al c.d. nickname tanto usato in chat come nell'uso anche di lettere di posta elettronica, purché soddisfi i requisiti appena elencati;
b. il diritto all'immagine, nel senso che è vietato esporre o pubblicare l'immagine altrui senza il consenso della persona ritratta, salvo che non si tratti di persona notoria oppure che l'immagine sia stata pubblicata nel contesto di un avvenimento svoltosi in pubblico e sempre che la pubblicazione non rechi pregiudizio alla dignità della persona;
c. il diritto all'onore (cioè il sentimento che l'individuo ha delle proprie qualità morali ovvero, in altri termini, della propria onorabilità, cioè dell'assenza di cause di disonore) e al decoro (cioè l'insieme delle altre qualità e condizioni che, come la dignità fisica, intellettuale o professionale, concorrono a costituire il valore sociale dell'individuo);
d. il diritto all'identità della persona. Diritto individuato recentemente dalla giurisprudenza, definito come il diritto a che non sia travisata la propria immagine politica, etica o sociale con l'attribuzione di azioni non compiute dal soggetto o di convinzioni da lui non professate;
e. il diritto alla riservatezza. Anche se nel codice civile non vi sono norme specifiche in materia, recentemente si è fatta spazio l'idea dell'esistenza di un vero diritto alla riservatezza. Già l'art. 2 della Costituzione prevede che "La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo nelle formazioni sociali ove si svolge la sua personalità".
Questa espressione, per quanto generale, costituisce il fondamento del diritto alla riservatezza, che tende appunto a preservare all'individuo un ambiente nel quale si svolge la sua personalità immune da intrusioni degli altri. L'art. 8 della Convenzione europea dei diritti dell'uomo testualmente tutela poi il rispetto alla vita privata e familiare; e vi sono altre norme che stabiliscono limiti all'uso di notizie relative al singolo, alla riproduzione di scritti personali, di immagini, ecc. Quando si parla di riservatezza in questo senso si allude a una delle due figure della riservatezza medesima: quella che riguarda il singolo fra le pareti di casa, o in ambiente privato, intimo, riservato. L'altro aspetto riguarda, invece, il controllo sulla circolazione delle informazioni personali, assunte da privati o da enti pubblici per conto dei singoli. Insomma, le due facce della riservatezza sono il diritto

all'anonimato e quello a non essere interferiti nella propria sfera personale. In quest'ultimo senso parliamo dell'attacco che lo spamming fa alla riservatezza personale di ognuno;
f. il diritto di libertà informatica. Diritto coniato dal compianto Vittorio Frosini [9] e inteso come "nuovo diritto soggettivo di libertà personale, sconosciuto alle età precedenti". Diritto che, inizialmente, era visto come facoltà dell'utente di non essere vittima di aggressioni alla propria riservatezza ("libertà da"), ma che oggi è da inquadrare nella "libertà di" fruire degli strumenti tecnologico-informatici, vivendo in maniera attiva il passaggio all'era dell'Information Technology. Esso è un "diritto di partecipazione alla società virtuale che è stata generata dall'avvento degli elaboratori elettronici nella società tecnologica".
Riprendendo le fila del discorso, fin qui si sono analizzati i problemi che lo spamming causa ai "normali" navigatori della Rete: l'invasione nella sfera privata della riservatezza personale. Questo fenomeno, però, è sempre più utilizzato per ledere gli interessi di altri soggetti, che, come i singoli navigatori, operano attivamente su Internet: le aziende. In molti casi, gli spammers, per arrecare danno a determinate società, spediscono le e-mail in modo tale da farle sembrare inviate proprio da quella società presa di mira. Così questi soggetti raggiungono contemporaneamente due risultati. In primo luogo, camuffano la propria identità, inserendo mittenti di altri soggetti; in secondo luogo, poi, arrecano pregiudizi economici a quelle aziende che, da un giorno all'altro, si ritrovano a essere catalogate come spammer.

Questo si chiama identity theft, o furto di identità, e porta molto spesso alla conseguenza che gli indirizzi di posta elettronica di quella determinata società vengano inseriti nelle c.d. black lists e che non arrivino mai ai propri clienti, perché intercettate e bloccate come spam [10].

SPAMMING E FURTI DI IDENTITÀ

Oggi le potenziali aggressioni del diritto all'identità personale non provengono esclusivamente da atti, fisici o immateriali, che comportano un'invasione della propria sfera privata. L'evoluzione tecnologica, infatti, se, da un lato, ha reso sempre più semplici e accessibili i meccanismi attraverso i quali la pretesa di solitudine dell'individuo tende a essere compressa, dall'altro, ha offerto forme di protezione e di prevenzione dalle intrusioni indesiderate, che consentono di risolvere o, quanto meno, di attenuare in radice tale fenomeno. Cosicché diventa essenziale non tanto evitare che altri violino il pur diritto fondamentale di essere lasciati soli, quanto consentire che ogni individuo possa disporre di un agile diritto di controllo, rispetto alle tante informazioni di carattere personale che altri possano aver assunto. Difatti, nell'attuale era tecnologica le caratteristiche personali di un

individuo possono essere tranquillamente scisse e fatte confluire in diverse banche di dati, ciascuna di esse contraddistinta da una specifica finalità.

Su tale presupposto può essere facilmente ricostruita la già citata "persona elettronica", attraverso le tante tracce che lascia negli elaboratori, che annotano e raccolgono informazioni sul suo conto. Con l'evoluzione tecnologica, dunque, non solo i nostri dati personali vivono disseminati nei database della Rete e dei nostri fornitori di beni e servizi, ma d'ora in avanti anche quelli più sensibili. Di certo le misure di sicurezza che si andranno ad adottare saranno studiate in modo tale da rendere più sicura che mai la gestione di dati altamente delicati, ma non si può fare a meno di notare una nuova "visione" della corporeità umana.

A questa disseminazione di informazioni personalissime corrisponde, infatti, una visione del corpo altrettanto frammentata, che elide l'unicità dell'uomo, dividendolo semplicemente in parti a sé stanti: "Impronte digitali, geometria della mano o delle dita o dell'orecchio, iride, retina, tratti del volto, odori, voce, firma, uso di una tastiera, andatura, Dna. Si ricorre sempre più frequentemente a questi dati biometrici, non solo per finalità d'identificazione o come chiave per l'accesso a diversi servizi, ma anche come elementi per classificazioni permanenti, per controlli ulteriori rispetto al momento dell'identificazione o dell'autenticazione/verifica, cioè della conferma di una identità" [11].

Nella Società dell'Informazione il corpo diventa un "insieme di dati", una metafora della Società globalizzata. Se la tendenza è questa, dunque, l'uomo (visto sia come unità a sé stante sia come sue parti separate) sarà sempre più catalogato come un "bene interconnesso", una sorta di alter ego virtuale, protocollato per rientrare nella "rete" comunicativa della Società.

La disponibilità dell'uomo come "bene" nelle mani altrui, unita a questo processo di smembramento del corpo e di "mercificazione" di ogni singolo nostro dato, ci porta al rischio di una pericolosa perdita di identità personale. L'uomo perde la propria identità, non ha più contorni definiti e diventa una "astrazione del cyberspazio" [12]. La conseguenza sarà una maggiore possibilità di controllo sociale, effettuabile attraverso infiniti mezzi. Fra quelli più innovativi e fantasiosi vi sono le installazioni di chip sotto pelle, che possono assolvere a diverse funzioni (effettuare pagamenti senza l'uso dei "classici" strumenti, essere identificato in una azienda, in un ospedale, ecc.).

"La sorveglianza sociale si affida così a una sorta di guinzaglio elettronico. Il corpo umano viene assimilato a un qualsiasi oggetto in movimento, controllabile a distanza con una tecnologia satellitare o utilizzando le radiofrequenze. Se il corpo può diventare una password, le tecnologie della localizzazione stanno facendo nascere una networked person". Proprio in merito all'esigenza di assicurare una forte tutela dei diritti e delle libertà delle persone, con particolare riferimento all'identità personale e alla vita privata degli individui, che utilizzano le reti telematiche, sono destinati a svolgere un ruolo determinante i codici deontologici e di buona condotta previsti da ultimo dal D.lgs. 30 giugno 2003, n. 196 (Codice per la protezione dei dati personali).

Le diverse questioni emerse nella materia in esame confermano peraltro la necessità di una cooperazione internazionale, anche in ragione del recepimento in Italia del principio di stabilimento, che può limitare il potere di intervento dell'Autorità Garante per la tutela dei dati personali rispetto ai trattamenti di dati personali effettuati da soggetti situati all'estero.

Sul punto, in Italia, il recente Codice per la protezione dei dati personali ha compiuto una ricognizione innovativa delle preesistenti norme sul trattamento dei dati nel settore delle telecomunicazioni (D.lgs. n. 171/1998, come modificato dal d.lgs. n. 467/2001), completando nello stesso tempo il recepimento della direttiva n. 2002/58/CE, relativa alla tutela della vita privata nel settore delle comunicazioni elettroniche. La disciplina introdotta in materia dal Codice, riproponendo un criterio già presente nella normativa comunitaria, adotta un approccio "tecnologicamente neutro", ossia valido e applicabile a tutte le forme di comunicazione elettronica, a prescindere dal mezzo tecnico utilizzato.

Naturalmente rimane il rischio che la diffusione dei documenti elettronici, come la Carta Nazionale dei Servizi e l'interconnessione di archivi informatici, possa comportare una riduzione dei diritti della persona e della riservatezza dei dati personali. Ciò anche in considerazione del fatto che, su questi profili, l'Italia non è dotata di una legislazione in tutto idonea a contemperare le esigenze di semplificazione e razionalizzazione dell'attività economica e commerciale con quelle di tutela della persona, anche in attuazione delle prescrizioni e dei principi generali già contenuti nella normativa comunitaria.

Al riguardo, l'Autorità Garante per la tutela dei dati personali, nell'esercizio della funzione consultiva di cui è titolare, ha più volte segnalato, negli anni precedenti, la necessità di individuare con maggiore attenzione e proporzionalità la tipologia dei dati da inserire nei documenti elettronici,

i soggetti che possono eventualmente accedere alle varie categorie di dati e le garanzie per gli interessati.

Un tipo di frode, ideato allo scopo di rubare l'identità di un utente, che si sta diffondendo in maniera davvero preoccupante è il phishing. Si tratta di una tecnica in base alla quale una persona malintenzionata cerca di appropriarsi di informazioni quali numeri di carta di credito, password, informazioni relative ad account o altre informazioni personali, convincendo l'utente a fornirgliele con falsi pretesti. Il phishing viene generalmente attuato tramite posta indesiderata o finestre a comparsa. Il phishing viene messo in atto da un utente malintenzionato che invia milioni di false e-mail che sembrano provenire da siti web noti o fidati come il sito della propria banca o della società di emissione della carta di credito. I messaggi di posta elettronica e i siti web in cui l'utente viene spesso indirizzato per loro tramite sembrano sufficientemente ufficiali da trarre in inganno molte persone sulla loro autenticità.

Ritenendo queste e-mail attendibili, gli utenti troppo spesso rispondono ingenuamente a richieste di numeri di carta di credito, password, informazioni su account e altre informazioni personali. Per far sembrare tali messaggi di posta elettronica ancora più veritieri, un esperto di contraffazione potrebbe inserirvi un collegamento, che apparentemente consente di accedere a un sito web autentico, ma che, di fatto, conduce a un sito contraffatto o persino una finestra a comparsa dall'aspetto identico al rispettivo sito ufficiale. Queste imitazioni sono spesso chiamate siti web c.d. "spoofed".

Una volta all'interno di uno di questi siti falsificati, è possibile immettere involontariamente informazioni ancora più personali, che verranno poi trasmesse direttamente all'autore del sito. Questi le utilizzerà per acquistare prodotti, richiedere una nuova carta di credito o sottrarre l'identità dell'utente. Quest'ultima "pratica" consistente nella clonazione di siti ufficiali viene comunemente denominata pharming e può essere attuata attraverso almeno due metodologie di attacco, a seconda che l'obiettivo primario sia il server Dns del provider oppure direttamente il Pc della vittima:

1. nel primo caso l'utente malintenzionato (cracker) opera, con sofisticate tecniche di intrusione, delle variazioni nei Server Dns del provider modificando gli abbinamenti tra il dominio e l'indirizzo Ip corrispondente a quel dominio. In questo modo gli utenti connessi a quel provider, pur digitando il corretto indirizzo Url, verranno inconsapevolmente reindirizzati a un server-trappola appositamente predisposto per carpire le informazioni.

Questo server trappola è ovviamente reperibile all'indirizzo Ip inserito dal cracker e l'aspetto del sito è esteticamente simile a quello vero.

2. nel secondo caso l'utente malintenzionato (cracker) opera, con l'ausilio di programmi trojan o tramite altro accesso diretto, una variazione nel personal computer della vittima. Per esempio, nei sistemi basati sul sistema operativo Windows, modificando il file hosts presente nella directory "C:\windows\system32\drivers\etc". Qui possono essere inseriti o modificati gli abbinamenti tra il dominio interessato (per esempio, paypal.com) e l'indirizzo Ip corrispondente a quel dominio. In questo modo la vittima che ha il file hosts modificato, pur digitando il corretto indirizzo Url nel proprio browser, verrà reindirizzata verso un server appositamente predisposto per carpire le informazioni. Un altro metodo consiste nel modificare direttamente nel registro di sistema i server Dns predefiniti. In questo modo l'utente - senza rendersene conto - non utilizzerà più i Dns del proprio Internet Service Provider, bensì quelli del cracker, dove ovviamente alcuni abbinamenti fra dominio e indirizzo Ip saranno stati alterati.

In tutto questo processo nulla può far ipotizzare alla vittima di essere connessa a un server-trappola se quest'ultimo è perfettamente somigliante a quello vero. Il cracker utilizzerà quindi a proprio beneficio i dati inseriti dalla vittima nel server "clone".

Da un punto di vista giuridico, il fattore più evidente sia nel caso del phishing sia in quello del pharming è il furto d'identità. Già da tempo il Garante sta esaminando questo aspetto con viva preoccupazione, ponendo la sua attenzione in tutti quei settori particolarmente delicati collegati alle nuove tecnologie, come le manipolazioni genetiche e l'utilizzo dei sistemi biometrici nel campo della sicurezza [13]. Di fronte alla rapida ascesa di tali metodologie il Garante sta assumendo un atteggiamento particolarmente rigido.

Spesso le finalità di identificazione, sorveglianza, sicurezza delle transazioni non possono giustificare qualsiasi utilizzazione del corpo umano, resa possibile dall'innovazione tecnologica. Vanno garantiti sempre il rispetto della dignità della persona, il rispetto dell'identità personale, il rispetto dei principi di finalità e di proporzionalità e, infine, la necessaria attenzione per gli effetti cosiddetti imprevisti o indesiderati e che, invece, spesso sono conseguenze determinate da analisi incomplete o troppo interessate delle tecnologie alle quali si intende ricorrere.

Ciò che maggiormente preoccupa è che il problema della protezione dell'identità dai suoi possibili "furti" (già imponente nel settore del commercio elettronico e che esige cautele particolari per le impronte digitali) con il phishing si estende ad altri settori, coinvolgendo in particolar modo il mondo bancario, postale e assicurativo, in breve tutto il settore economico-finanziario [14].

Ma il phishing, come si è detto in precedenza, è innanzitutto una vera e propria frode di carattere informatico. Si ricorda che l'art. 10 della Legge 547/1993 ha inserito nel corpo delle norme penali in tema di truffa la specifica ipotesi di frode informatica. La ratio della disposizione deriva dalla difficoltà di applicazione della fattispecie tradizionale di truffa (art. 640 codice penale), nel caso in cui la medesima venga perpetrata attraverso l'impiego di tecniche informatiche o telematiche. Si tratta di una fattispecie mediata dall'ordinamento penale tedesco e formulata in modo generico e vago. è da intendersi nel senso più ampio, tale da abbracciare ogni possibile intervento sia sull'input sia sul programma sia sulla consolle. Tale fattispecie ha confini così dilatati che, attraverso la previsione della condotta di "utilizzazione non autorizzata di dati, finalizzata a procurare a sé o ad altri un vantaggio patrimoniale illecito" e di "danneggiamento" del patrimonio altrui influendo sul risultato di un procedimento di elaborazione automatica di dati, è possibile punire gli "abusi" realizzati attraverso il Bancomat.

L'art. 640-ter c. p. sanziona con la pena della reclusione da 6 mesi a 3 anni e con la multa da euro 51,65 a euro 1032,91 chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno. La struttura è per certi versi analoga a quella dell'art. 640 c. p., ma la disposizione in esame non prevede il requisito della induzione in errore di taluno: l'unanime interpretazione della giurisprudenza, infatti, è nel senso di ritenere che il pronome personale ("inducendo taluno in errore") debba riferirsi a una persona fisica.

La nuova norma, quindi, assume importanza laddove non sia configurabile un soggetto "vittima" della induzione in errore: situazione che si verifica puntualmente nel caso specifico, poiché l'autore ha come interlocutore il solo elaboratore. Per superare l'ostacolo giuridico all'applicazione della fattispecie per la violazione del divieto di analogia in materia penale, il legislatore ha descritto la condotta ex art. 640-ter c. p. in termini di "alterazione in qualsiasi modo" effettuata del funzionamento del sistema, o di intervento senza diritto con qualsiasi modalità su dati o programmi contenuti in un sistema informatico. La condotta difetta sul piano della determinatezza, che pure è

requisito essenziale nella creazione delle fattispecie penali. Le caratteristiche della "alterazione", infatti, non sono definite né circoscritte, perciò la condotta stessa non è facilmente qualificabile.

La necessità della induzione in errore di taluno è superata, mentre il disvalore della fattispecie si incentra nella qualificazione della condotta di alterazione del sistema, definita come alterazione compiuta "senza diritto", ovvero non autorizzata dal "titolare del sistema" o da colui che ne è comunque responsabile.

NOTE

[1] La "rete dell'agenzia dei progetti di ricerca avanzata" (Advanced Research Projects Agency Network, Arpanet). Realizzata nel 1969 dal Darpa (Defence Avanced Research Project Agency) del Dipartimento della Difesa degli Stati Uniti, Arpanet aveva l'ambizioso compito di aumentare in maniera radicale il livello di sicurezza delle comunicazioni militari.

[2] CELENTANO (a cura di), Manuale Breve di Informatica per Avvocati, Torino, 2007.

[3] Il primo caso clamoroso e documentato di spam di posta elettronica risale al 1 maggio 1978 quando una mail fu inviata da un certo Gary Thuerk, un impiegato del settore marketing della Dec (Digital Equipment Corporation), a ben 593 indirizzi di posta elettronica. (TEMPLETON, Origin of the term "spam" to mean net abuse, reperibile alla Url http://www.templetons.com/brad/spamterm.html).

[4] Rapporto Ocse, redatto per il Seminario in materia di spam del 2-3 febbraio 2004, Background Paper For The OECD Workshop On Spam, DSTI/ICCP(2003)10/FINAL.

[5] Analizzando l'attività dei siti di e-mail anonime, si potrebbe ritenere che essa implichi due distinte tipologie di spamming. La prima, originata dall'utente, è solamente marginale e meramente collegata al messaggio che il mittente vuol far pervenire al destinatario (la pubblicità, come “prezzo” per l'utilizzo del servizio di anonimato). La seconda, invece, è la vera attività di spamming, poiché, qualora il sito A memorizzasse tutti gli indirizzi di posta elettronica dei destinatari e li utilizzasse per inviare materiale a scopo promozionale, vi sarebbe sicuramente un'attività di spamming in senso stretto. Per quanto concerne la prima tipologia, però, si può notare che anch'essa è propriamente una attività di spamming, (anche se realizzata in maniera originale – potrebbe dire qualcuno – , e cioè non mediante la spedizione diretta di materiale promozionale via

e-mail). Se lo spamming consiste nel far pervenire a un ignaro utente pubblicità di beni e/o servizi, senza che questi ne abbia chiesto l'invio, dovrebbe essere indifferente il mezzo con il quale essa perviene. Dunque, ogni volta che ciascuno di noi è “costretto” a vedere un determinato tipo di pubblicità, è leso il nostro diritto alla riservatezza.

[6] Cfr. in questo Quaderno (2004), La rete contro lo spam: che cos’è, come combatterlo.

[7] Si calcola che, se nel 2004 lo spam era quasi un terzo del totale di e-mail circolanti, adesso è la metà. Il numero di email spazzatura è quasi raddoppiato in tre anni (fonte Idc).

[8] DE ROSA, La formazione di regole giuridiche per il cyberspazio, in Dir. Inf., 2003, p. 377.

[9] FROSINI, L’orizzonte giuridico in Internet, in Dir. Inf., 2002, p. 271.

[10] Negli anni Novanta, il modo più diffuso per inviare spam era di servirsi dei c.d. open mail relay, ossia di server di posta elettronica (nel gergo tecnico, Mail Transfer Agent) configurati per ricevere e inviare messaggi da e verso qualsiasi indirizzo di e-mail. Per contrastare questi abusi venne escogitato il meccanismo del Dnsbl (Dns Black List), ancora oggi attivo in diverse varianti, che consisteva nel pubblicare una lista di indirizzi IP marcati come non affidabili e quindi utilizzabili eventualmente dai server di posta elettronica per bloccare messaggi di posta elettronica provenienti da tali indirizzi. Con la sparizione degli open mail relay, gli spammers iniziarono a servirsi dei c.d. open proxy che consentivano di fare da tramite veicolando il traffico generato dei client di posta elettronica e nascondendo di fatto l’indirizzo Ip del computer di origine. Gli anni 2000 hanno visto la diffusione dei virus spammer tra cui quelli appartenenti alle famose famiglie Sobig e Mimail. Servendosi di computer infettati da uno di questi virus, la cui minaccia è sempre presente grazie alle numerose e a volte imprevedibili varianti, gli spammers sono in grado di agire nascondendo completamente le proprie tracce e di procurarsi nuovi indirizzi di e-mail attingendo direttamente dalle rubriche degli utenti e dalle cartelle locali della posta inviata e ricevuta.

[11] RODOTÀ, Trasformazioni del corpo, in Pol. dir., n. 1/06, p. 6-7.

[12] RODOTÀ, Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali, in Riv. crit. dir. priv., 1997, 4, p. 605.

[13] Come è noto le tecnologie biometriche, consentono, mediante l'uso di specifici software e apparecchiature informatiche, il riconoscimento di un individuo attraverso dati fisici ricavati dall'analisi delle impronte digitali, della morfologia facciale e dal riconoscimento palmare. In particolare queste tecnologie sofisticate, riconosciute anche dal legislatore italiano, utilizzano delle chiavi c.d. biometriche intese come la sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente. In tema di accessi informatici i sistemi biometrici rappresentano la ricerca più avanzata nel campo della sicurezza. Alcune caratteristiche fisiche dell'utente autorizzato all'accesso, vengono memorizzate dal computer e confrontate con quelle della persona che accede.

[14] Del tutto drammatiche sarebbero poi le conseguenze, se il furto d'identità dovesse riguardare materiale che consenta di ottenere informazioni genetiche. Se, infatti, grandi sono le opportunità offerte dalla genetica, altrettanto grandi sono i rischi di utilizzazioni di tali dati, che possono determinare discriminazioni nell'accesso al lavoro o al credito, nella conclusione di contratti di assicurazione vita o malattia, o attraverso forme di schedatura genetica di massa. Insomma, come giustamente sottolineato dall'Autorità, possono nascere nuove disuguaglianze e soprattutto in campo internazionale si fa molta attenzione a questo aspetto. È necessario, quindi, controllare la legittimità di ogni forma di trattamento dei dati genetici e approntare un sistema di tutela dei dati necessario, per consentire a tutti di godere al massimo dei benefici della ricerca genetica. Anche in questo settore l'avvento di Internet ha complicato ulteriormente le cose e la diffusione dell'offerta di test genetici tramite la Rete costituisce un drammatico esempio.

ENZO FOGLIANI

Internet governance e tutela dell'utente in Italia

Enzo Fogliani, nato a Milano nel 1958, avvocato cassazionista, docente di informatica giuridica presso l'università di Udine, per la quale ha organizzato convegni sulle problematiche giuridiche di Internet. Consigliere di ISOC italia. Nel 1998 è fra i fondatori della Naming Authority, nel cui Comitato esecutivo ha svolto la propria attività dal 1998 al 2005. Membro dal 2005 della Commissione per le Regole del Registro del ccTLD .it, su designazione di Isoc Italia.
Autore di numerose pubblicazioni giuridiche e relatore in convegni giuridici. Esperto di procedure di riassegnazione. Arbitro accreditato per le procedure di risoluzione delle dispute per i domini .it e .eu.

IL SISTEMA PRECEDENTE: NAMING AUTHORITY E REGISTRATION AUTHORITY

Il sistema su cui si era retto sino agli inizi del 2004 il governo di Internet in Italia aveva avuto origine nel 1997, allorché i componenti del gruppo ITA-PE (che riuniva in una lista di discussione i primi provider - maintainer e gli appassionati di Internet e che sulla base del rough consensum aveva predisposto le prime regole per il funzionamento di Internet in Italia) avevano deciso di formalizzare la propria posizione di ente normatore che avevano svolto di fatto sino a quel momento.

A tal fine era stato nominato un gruppo di lavoro, che nell'ottobre 1998 sottopose all'assemblea del gruppo ITA-PE lo statuto predisposto in un anno di lavoro. Con la sua approvazione nasceva ufficialmente la Naming Authority italiana, la quale, con l'accordo della Registration Authority (che pure in essa aveva i propri rappresentanti) assumeva le funzioni normative per il ccTLD .it.

Nel settembre 1999 il comitato esecutivo eletto l'anno precedente contestualmente alla approvazione dello statuto sottoponeva all'assemblea della Naming Authority le nuove regole di naming, destinate a segnare una svolta fondamentale nella storia dell'Internet italiana. Una volta approvate, le nuove regole entrarono in vigore il 15 dicembre 1999.

Le procedure di registrazione dei domini venivano semplificate mediante la previsione, fra le altre cose, della possibilità di autocertificazione. La legittimazione alla registrazione nel ccTLD .it veniva estesa dai soli cittadini italiani a tutti i soggetti facenti parte della unione europea; cadeva il

limite di un solo nome a dominio per le imprese e gli enti commerciali; anche le persone fisiche erano ammesse a registrare nomi a dominio, seppur uno ciascuna.

La bontà delle nuove regole era confermata dall'enorme incremento dei nomi a dominio registrati nel ccTLD .it, che dai circa novantamila della fine del 1999 passavano ai circa cinquecentomila della metà del 2000. Il sistema delle nuove regole veniva poi completato nell'agosto del 2000 dall'introduzione delle "procedure di riassegnazione", procedimenti alternativi per la risoluzione delle dispute sui nomi a dominio, particolarmente efficaci per contrastare il cybersquatting.

Il governo di Internet italiana così strutturato rispettava sostanzialmente a grandi linee i classici canoni di tripartizione dei poteri delle democrazie occidentali. La Registration Authority, cui spettava materialmente la gestione del registro e l'assegnazione dei nomi a dominio, rappresentava il potere esecutivo.

La Naming Authority svolgeva la funzione legislativa e gli enti conduttori (che si occupavano delle procedure di riassegnazione) la funzione giudiziaria. Quest'ultima, peraltro, aveva efficacia limitata, in quanto la proposta di garantire gli utenti con un sistema di arbitrato obbligatorio per le questioni dei nomi a dominio era stata disattesa, con conseguente proliferazione di fenomeni di accaparramento, solo in un secondo momento contrastati (e in maniera molto meno efficace) dalle procedure di riassegnazione.

Le regole di naming predisposte dalla Naming Authority acquistavano efficacia vincolante per la Registration Authority, i maintainer e gli assegnatari dei nomi a dominio in virtù dell'espresso richiamo contenuto nel contratto fra Registration Authority ed i singoli maintainer, e dell'impegno a rispettarle che gli utenti assegnatari dei nomi a dominio sottoscrivevano firmando la "lettera di assunzione di responsabilità" necessaria per la registrazione.

La Naming Authority funzionava su basi democratiche. Di essa facevano parte di diritto i maintainer, nonché, a richiesta, tecnici, professionisti o semplici privati che si interessassero di Internet e fossero interessati a dare il loro contributo. L'assemblea della Naming Authority si riuniva almeno una volta all'anno, eleggendo il proprio presidente ed il Comitato esecutivo. A quest'ultimo, integrato dai rappresentanti della Registration Authority e di eventuali altri esperti cooptati per scopi specifici, spettava le redazione delle regole di naming. Il presidente della Naming Authority svolgeva funzioni di coordinamento, di controllo e di garanzia, sia sul Comitato esecutivo, sia sugli

Enti Conduttori delle procedure di riassegnazione dei nomi a dominio.

Lo stesso successo delle nuove regole (e dei domini .it cui si riferivano) fu probabilmente la causa prima dell'inizio della decadenza del sistema imperniato sulla Naming Authority. I nuovi maintainer, nati dopo la liberalizzazione, poco si curarono di iscriversi alla Naming Authority per partecipare alla predisposizione delle norme di un sistema che sostanzialmente funzionava in modo soddisfacente. Nel corso del tempo, quindi, la Naming Authority, pur ampliando il novero dei propri associati con persone provenienti dagli ambienti più vari, perse la sua caratteristica di ente rappresentativo della maggioranza dei maintainer, che costituivano la controparte contrattuale della Registration Authority per la registrazione dei nomi a dominio.

La Naming Authority, priva di entrate e di un proprio bilancio, dipendente dal volontariato dei propri associati, si trovò nel mezzo di rilevanti interessi economici, senza d'altra parte riuscire a suggerire rotte di sviluppo del sistema diverse da quelle dirette al settore pubblica amministrazione e a quello commerciale che principalmente Registration Authority e maintainer perseguivano.

La sua funzione di ente che redigeva le norme che di fatto costituivano le clausole del contratto fra i maintainer e la Registration Authority la resero un elemento scomodo sia per la Registration Authority, che per i grandi maintainer.

La prima non era in grado di far riflettere anche nelle regole per la registrazione dei nomi a dominio in sede contrattuale le proprie esigenze nascenti dalla situazione di monopolista di fatto cui si trovava non certo per propria scelta, ma per la stessa struttura tecnica e giuridica di Internet.

I secondi, pur sostenendo gran parte dei costi del funzionamento del sistema, non erano in grado di far valere la propria forza contrattuale ed economica nella formulazione delle regole.

Da parte loro, i maintainer di minor peso economico apparivano preoccupati più dei problemi di concorrenza commerciale fra loro che di favorire uno sviluppo armonico e sociale della rete; mentre i rimanenti componenti della Naming Authority, privi di peso economico nell'ambito del rapporto contrattuale fra Registration Authority e maintainer, ben poco potevano incidere sulla formulazione delle norme.

La situazione favorì negli anni 2000 e 2001 alcuni tentativi della classe politica di attrarre la registrazione dei nomi a dominio nell'ambito del diritto pubblico, che si sarebbe voluta attuare mediante la trasformazione della Registration Authority in amministrazione statale. Respinti tali tentativi dalla comunità Internet nazionale, a partire dalla fine del 2002 la Registration Authority ritenne non più sostenibile l'ormai vischioso ed inefficiente sistema decisionale della Naming Authority ed iniziò a rivendicare a proprio favore la funzione normativa che quest'ultima aveva fino ad allora esercitato.

Nella seconda metà del 2003, in prossimità della scadenza del contratto che legava i maintainer e la Registration Authority alle regole di naming predisposte dalla Naming Authority, la Registration Authority fece sapere che dall'inizio del 2004 non si sarebbe ritenuta più vincolata alla Naming Authority. Cosa che è poi regolarmente avvenuta, con il benestare dei grossi maintainer e di buona parte dei vertici della Naming Authority stessa.

Il nuovo contratto predisposto dalla Registration Authority a far data dal 1 gennaio 2004 affidò dunque al solo Registro la potestà normativa in tema di regole di naming, senza alcun cenno alla vecchia Naming Authority. Quest'ultima, che pure tanta parte aveva avuto nello sviluppo di Internet in Italia, si sciolse poi mestamente il 12 luglio 2005, e di essa non resta in vita che la gloriosa lista di discussione ITA-PE, tuttora attiva.

IL NUOVO SISTEMA: LA COMMISSIONE PER LE REGOLE DEL REGISTRO

Il vecchio sistema basato sul dualismo Registration Authority e Naming Authority è stato dunque sostituito a far data dal 2004 da un nuovo sistema nel quale l'Internet governance del ccTLD .it è accentrata nel "Registro". Protagonista centrale del riformato ordinamento di Internet in Italia è il "Registro del ccTLD .it", nuovo nome assunto dalla Registration Authority italiana.

Nel suo ambito è stata costituita una "Commissione per le regole e procedure tecniche del Registro del ccTLD "it" (Commissione Regole), con funzioni consultive, il cui compito è quello di proporre al Direttore del Registro le norme per l'assegnazione e la gestione dei nomi a dominio italiani.

La Commissione Regole è composta da sei membri designati da alcune associazioni o gruppi che il Registro ritiene rappresentative della LIC (Local Internet Community) italiana, da due membri nominati dallo IIT-CNR (in sostanza, dal Direttore del Registro stesso) e da uno nominato dal Consortium GARR. Il Direttore del Registro può inoltre nominare membri della commissione altre

due persone "che per specifici titoli possano garantire un elevato apporto di conoscenze ed esperienze nell'Internet" ed integrarla con ulteriori 5 membri "scelti fra esponenti governativi o di organismi pubblici indicati dai Ministeri e dalle Autorità competenti". I membri della commissione durano in carica per un anno a far data dalla nomina e possono essere riconfermati.

Al suo interno la Commissione elegge un Presidente, che provvede alla convocazione delle riunioni della Commissione e ne controlla la trasparenza degli atti. Le decisioni della Commissione sono inviate entro dieci giorni a cura del Presidente al Direttore del Registro, il quale, se ritiene di darvi attuazione, entro ulteriori quindici giorni comunica alla Commissione i tempi in cui darà attuazione a quanto deliberato. Se invece non ritiene opportuno attuare quanto deciso dalla Commissione, il Direttore del Registro può chiedere un riesame della questione.

La decisione sul momento in cui dare esecuzione alle modifiche alle regole suggerite dalla commissione spetta al Direttore del Registro, il quale peraltro può anche assumere decisioni urgenti in materia di regole e procedure tecniche senza il previo parere della Commissione. Su tali decisioni d'urgenza la Commissione delibera alla prima riunione successiva, senza che peraltro il suo parere sia vincolante per il Direttore del Registro o possa inficiare le decisioni da questi prese. I componenti della Commissione sono vincolati al più stretto riserbo circa i lavori. Essendo la Commissione consultiva, le regole che essi predispongono non hanno valore vincolante per il Registro se non dopo la loro approvazione da parte del Direttore del Registro, che sull'argomento gode della massima discrezionalità.

La Commissione per le regole ha iniziato i propri lavori il 16 marzo 2004, modificando le precedenti regole di naming per adeguarle alla nuova struttura della Internet governance introdotta dal Registro.

La nuova versione delle regole è entrata in vigore il 2 agosto 2004. Successivamente, la Commissione ha lavorato ad una nuova versione delle regole che adeguasse le modalità tecniche di registrazione a quelle in uso in altri TLD, mediante la possibilità per il maintainer (denominato nel nuovo sistema "registrar") di provvedere direttamente alle modifiche del data base dei nomi a dominio. Le nuove regole dovrebbero prevedere una modalità di registrazione cosiddetta "asincrona", sostanzialmente analoga a quella attuale, ed una modalità di registrazione cosiddetta "sincrona", analoga a quella, priva di documentazione cartacea, utilizzata per il .eu.

Alla fine del 2006, dopo alcuni rinvii, è stato quindi emanato il nuovo Regolamento per l'assegnazione e la gestione dei domini nel ccTLD "it", che peraltro prevede al momento soltanto la modalità di registrazione asincrona. Le nuove regole per la registrazione asincrona sono in vigore dal 28 febbraio 2007, mentre al momento non è possibile fare previsioni circa l'implementazione delle modalità di registrazione sincrona.

LE PROCEDURE ALTERNATIVE DI RISOLUZIONE DELLE DISPUTE

Nel sistema dei nomi a dominio, in relazione alla tutela dell'utente possono individuarsi due settori disciplinati dalle norme predisposte dalla Commissione per le regole del Registro: il settore della tutela dell'utente nei confronti di altri utenti per violazioni di diritti conseguenti a registrazioni abusive di nomi a dominio, e il settore della tutela dell'utente nei confronti di Registro e maintainer. Per quanto riguarda il primo aspetto, il sistema italiano si è da tempo adeguato a quello introdotto da ICANN nel 1999 per combattere il cybersquatting, basato sulle MAP (Mandatory Administrative Proceedings o, all'italiana, procedure di riassegnazione).

È inoltre stato previsto un vero e proprio procedimento arbitrale, che peraltro ad oggi ha avuto scarsissimo successo. Le procedure di riassegnazione sono state introdotte in Italia dalla Naming Authority nel 2000 seguendo sostanzialmente il modello di ICANN. Esse sono passate indenni nel cambiamento di regime che ha portato alla creazione della Commissione per le regole e sono state riprodotte sostanzialmente immutate anche nel nuovo Regolamento entrato in vigore il 28 febbraio 2007, che di fatto ha modificato solo le modalità di accreditamento dei PSRD (Prestatori dei servizi di risoluzione delle dispute), gli enti cui è affidata la gestione del contenzioso, che fungono da "cancelleria" per gli esperti cui sono affidate le decisioni. I PSRD sono abilitati alla gestione delle procedure dal Registro, su parere positivo della Commissione per le regole, previa verifica dell'esistenza di una lista di almeno 15 esperti disponibili a rendere le decisioni nelle procedure, di un sito web su cui pubblicarle, di una stabile organizzazione per gestirle.

L'abilitazione ha durata biennale ed è rinnovabile. Per poter operare, il PSRD deve dotarsi di assicurazione della responsabilità civile. Per prevenire l'abnorme proliferazione di PSRD che aveva caratterizzato il regime precedente, la Commissione per le regole ha deciso di limitare a 6 il numero massimo di PSRD. Secondo le norme che regolano le procedure di riassegnazione, un nome a dominio si considera registrato abusivamente e viene quindi riassegnato ad un terzo che lo reclami, quando sia dimostrato che: a) il nome a dominio è identico o di similitudine tale da indurre in confusione in relazione al suo nome o ad un marchio su cui egli vanta dei diritti; b) l'assegnatario

del nome a dominio non abbia diritti o legittimi interessi in relazione al suddetto dominio; c) il nome a dominio sia stato registrato e venga usato in malafede.
Il procedimento è piuttosto rapido e semplice. Il ricorrente (cioè colui che ritiene essergli stato sottratto illegittimamente un nome a dominio) presenta al PSRD prescelto il ricorso e la relativa documentazione, versando quanto previsto dalle tariffe in vigore per il procedimento. Il PSRD invia ricorso e documentazione all'assegnatario del nome a dominio contestato, invitandolo a far pervenire le proprie repliche e la documentazione a supporto delle sue difese.

Una volta ricevute le repliche (o scaduto inutilmente il termine di 25 giorni senza che l'assegnatario ne abbia inviate), il PSRD nomina l'esperto (o un collegio di tre esperti, a seconda delle indicazioni del ricorrente) scelto fra un elenco di persone selezionate dal PSRD stesso. La decisione deve essere emessa entro 15 giorni (aumentabili se le parti richiedono di scambiarsi ulteriori difese). Se l'esito è favorevole al ricorrente (ossia se viene disposta la riassegnazione del nome a dominio) il Registro attua la decisione, salvo che entro il termine di 15 giorni dalla comunicazione della decisione il soccombente non ricorra alla magistratura.

LE PROCEDURE DI RIASSEGNAZIONE

Le procedure di riassegnazione si inquadrano nell'ordinamento giuridico italiano. Per esplicita previsione del Regolamento, la procedura di riassegnazione italiana "non ha natura giurisdizionale, e come tale non preclude alle parti il ricorso, anche successivo, alla magistratura o all'arbitrato".

Essa si inserisce funzionalmente nell'ambito procedimentale della registrazione e più precisamente nell'ambito della verifica del titolo alla richiesta del nome a dominio. La procedura tende infatti ad accertare la rispondenza al vero della dichiarazione, contenuta nella lettera di assunzione di responsabilità, con la quale il richiedente il nome a dominio dichiara di avere titolo all'uso o disponibilità giuridica del nome a dominio richiesto e di non ledere con tale richiesta di registrazione diritti di terzi.

La circostanza che questo tipo di verifica non sia svolto d'ufficio, ma su sollecitazione ed in contraddittorio con un soggetto che assume leso un proprio diritto non muta la natura della procedura, che rimane pur sempre di tipo amministrativo; tanto che la procedura italiana non può essere intrapresa in pendenza di giudizio o di arbitrato sul nome a dominio contestato, e si interrompe nel caso un giudizio ordinario sia intrapreso durante il suo corso.

Le norme sulle procedure di riassegnazione hanno dunque carattere meramente procedimentale. Esse vincolano tutti gli assegnatari dei domini sotto il ccTLD .it in virtù del richiamo dinamico al Regolamento contenuto nella lettera di assunzione di responsabilità con cui è stato registrato il nome a dominio, richiamo che assoggetta l'assegnatario non solo al Regolamento vigente al momento della registrazione del dominio, ma anche alle sue future modifiche.

Come regole di carattere procedimentale, sulla base del principio "tempus regit actum", si applicano nella versione in vigore al momento del procedimento, indipendentemente dal momento in cui il nome a dominio è stato registrato o è stato sottoposto a contestazione. La scelta del PSRD cui sottoporre la contestazione del dominio è lasciata al ricorrente, il quale può anche scegliere se far decidere la controversia da un solo esperto o da un collegio di tre esperti.

L'atto introduttivo del procedimento deve essere presentato sia in versione cartacea che elettronica e deve contenere tutti gli elementi previsti dal Regolamento, pena la inammissibilità del ricorso. Non viene imposto un formulario specifico, anche se i PSRD suggeriscono in genere nel loro sito un modulo contenente tutti gli elementi previsti dalle norme. Il costo del procedimento è sostenuto interamente dal ricorrente e deve essere versato anticipatamente. All'esito positivo della procedura, il ricorrente potrà eventualmente adire al giudice ordinario per ottenere la condanna di chi aveva illegittimamente registrato il nome a dominio al rimborso delle spese per il procedimento.

Le norme prevedono esplicitamente che il costo della procedura non venga restituito al ricorrente, anche nel caso di successiva rinuncia al ricorso o nel caso in cui la procedura si interrompesse per uno dei casi previsti. Una volta ricevuto il ricorso via e-mail e in formato cartaceo, il PSRD provvede ad inviarlo per raccomandata all'assegnatario del nome a dominio contestato. Questi deve far pervenire le sue eventuali repliche e documenti entro 25 giorni. Il termine decorre dal momento in cui il ricorrente ha conoscenza del ricorso; momento che a tutti gli effetti viene considerato quello di inizio della procedura.

Ricevute le repliche o trascorso inutilmente il termine suddetto, il PSRD nomina l'esperto o il collegio giudicante fra gli esperti della propria lista, che decide sulla controversia entro 15 giorni dall'accettazione dell'incarico. Il termine per la decisione può essere prorogato nel caso in cui le parti chiedano di produrre ulteriori scritti difensivi o documenti. La decisione viene comunicata dal PSRD entro 4 giorni alle parti ed al Registro. Nel caso in cui il ricorso venga accolto, il Registro provvede al trasferimento del nome a dominio a meno che non riceva, entro 15 giorni dalla data in

cui gli è pervenuta la decisione, una comunicazione adeguatamente documentata da parte del resistente di aver iniziato un procedimento giudiziario in relazione al nome a dominio contestato.

L'introduzione di un tale giudizio blocca l'esecuzione della decisione e la riassegnazione del nome a dominio. Se invece nulla perviene al Registro entro tale periodo, il dominio viene revocato al precedente assegnatario ed il vincitore della procedura invitato ad esperire i necessari passi per ottenere la registrazione del dominio a suo favore.

Elemento essenziale su cui sono basate le decisioni per la riassegnazione del nome a dominio è la malafede nella registrazione e nel mantenimento del nome a dominio in contestazione da parte dell'assegnatario. Il regolamento prevede in via esemplificativa alcune circostanze ritenute indicative della malafede dell'assegnatario del nome a dominio. Esse sono:

a. circostanze che inducano a ritenere che il nome a dominio è stato registrato con lo scopo primario di vendere, cedere in uso o in altro modo trasferire il nome a dominio al ricorrente (che sia titolare dei diritti sul marchio o sul nome) o ad un suo concorrente, per un corrispettivo, monetario o meno, che sia superiore ai costi ragionevolmente sostenuti dal resistente per la registrazione ed il mantenimento del nome a dominio;
b. la circostanza che il dominio sia stato registrato dal resistente per impedire al titolare di identico marchio di registrare in proprio tale nome a dominio, ed esso sia utilizzato per attività in concorrenza con quella del ricorrente;
c. la circostanza che il nome a dominio sia stato registrato dal resistente con lo scopo primario di danneggiare gli affari di un concorrente o di usurpare nome e cognome del ricorrente;
d. la circostanza che, nell'uso del nome a dominio, esso sia stato intenzionalmente utilizzato per attrarre, a scopo di trarne profitto, utenti di Internet creando motivi di confusione con il marchio del ricorrente.

Tuttavia, il collegio può desumere la malafede nella registrazione e nel mantenimento del nome a dominio da qualsiasi altra circostanza emerga nel corso della procedura di riassegnazione; tanto che a volte la malafede è stata desunta dalla sola notorietà del marchio cui il nome a dominio in contestazione è identico.

Nel corso del tempo si sono quindi delineate con precisione alcune fattispecie tipiche ulteriori rispetto a quelle esemplificativamente previste dai regolamenti. Fra queste, possono citarsi il

cosiddetto "passive domain holding" ossia la mera registrazione di un nome a dominio identico al nome o al marchio altrui, senza che esso sia utilizzato in alcun modo; oppure il cosiddetto "pornosquatting", ossia l'utilizzo del nome a dominio registrato per localizzarvi un sito porno, oppure per ridirezionare l'utente su un sito pornografico di terzi, del tutto estranei alla operazione di cybersquatting. In altri casi, è stato ritenuto elemento indicativo della malafede l'indicazione al Registro, al momento della registrazione, di un nome o di un indirizzo falso da parte dell'assegnatario.

PROCEDURA DI RIASSEGNAZIONE E RICORSO ALLA MAGISTRATURA

Le procedure di riassegnazione rappresentano uno strumento alternativo al ricorso alla magistratura ordinaria allorché si lamenti una registrazione abusiva di un nome a dominio. Tuttavia, una controversia sottoposta a procedura di riassegnazione non necessariamente ha lo stesso esito che avrebbe se sottoposta alla magistratura ordinaria. Infatti, le norme sulla base delle quali sono decise le procedure di riassegnazione, da un lato sono principalmente volte a combattere il fenomeno del cybersquatting, dall'altro tengono conto delle peculiarità dell'ambiente Internet in cui ci si muove in misura maggiore di quanto non facciano le norme di legge applicate dal giudice ordinario.

Le procedure di riassegnazione hanno come punto centrale non tanto il diritto del ricorrente sul nome a dominio contestato, quanto la buona fede dell'assegnatario nella registrazione e nel mantenimento del nome a dominio. Non è infatti sufficiente per il ricorrente dimostrare di vantare un diritto al nome a dominio in contestazione, ma è necessario provare anche la malafede del resistente nella registrazione e nel mantenimento del nome a dominio. Il ricorrente deve infatti dimostrare che il nome a dominio contestato è identico o tale da indurre confusione rispetto ad un marchio su cui egli vanta diritti, o al proprio nome e cognome, e che il nome a dominio sia stato registrato e venga usato in mala fede.

Una volta provato dal ricorrente un proprio diritto sul nome a dominio, spetta al resistente provare di avere a sua volta un concorrente titolo o diritto sul nome a dominio stesso. Se non ci riesce, ed il ricorrente ha assolto agli oneri probatori che su di lui incombono, il dominio viene trasferito a chi lo ha contestato. Se invece il resistente prova di avere a sua volta un diritto o un titolo al nome a dominio (seppur concorrente con quello del ricorrente), il ricorso viene respinto.

Le procedure di riassegnazione prevedono che, anziché provare l'esistenza di un vero e proprio diritto sul nome a dominio contestato, il resistente possa provare alcune circostanze dimostrando

l'esistenza delle quali viene dato ingresso ad una presunzione juris et de jure che il resistente stesso abbia titolo al nome a dominio contestato; con la conseguenza che, in applicazione del principio prior in tempore potior in jure, nella concorrenza di più diritti sullo stesso nome a dominio viene preferito quello di chi per primo lo ha registrato.

Le circostanze alla cui prova il Regolamento fa conseguire la suddetta presunzione di diritto o titolo al nome a dominio a favore del resistente sono: (a) che prima di avere avuto notizia della contestazione il resistente abbia usato o si sia preparato oggettivamente ad usare in buona fede il nome a dominio o un nome ad esso corrispondente per offerta al pubblico di beni e servizi; oppure (b) che il resistente stesso sia conosciuto, personalmente, come associazione o ente commerciale, con il nome corrispondente al nome a dominio registrato, anche se non ne abbia registrato il relativo marchio; oppure (c) che del nome a dominio il ricorrente stia facendo un legittimo uso non commerciale, oppure commerciale senza l'intento di sviare la clientela del ricorrente o di violarne il marchio registrato.

Se da un lato il ricorrente è facilitato dalla previsione di circostanze specifiche che, se provate, assumono il valore di vere e proprie presunzioni nella prova della malafede, dall'altro il resistente ha a sua disposizione presunzioni juris et de jure che non trovano riscontro nelle norme che regolano il giudizio ordinario.

Non solo infatti nelle procedure di riassegnazione non ha alcun rilievo l'eventuale priorità del ricorrente rispetto al resistente nell'acquisto del diritto sul nome a dominio in contestazione, essendo rilevante soltanto la concorrente esistenza di un diritto del resistente, indipendentemente dal momento in cui tale diritto è sorto; ma tale diritto è ritenuto comunque esistente in presenza di determinate circostanze che, in un giudizio ordinario, sarebbero del tutto irrilevanti.

Quindi, mentre in un giudizio ordinario sarebbe sufficiente che il ricorrente dimostrasse un proprio diritto esclusivo (o comunque precedente a quello del resistente) sul nome a dominio, e la mala fede dell'assegnatario avrebbe importanza relativa (rilevando soltanto in relazione ad una eventuale richiesta di risarcimento del danno), nelle procedure di riassegnazione l'elemento soggettivo del resistente è punto fondamentale. Con la conseguenza che, in mancanza della dimostrazione della malafede nella registrazione e nel mantenimento del nome a dominio, anche chi vanti diritti di esclusiva su un nome a dominio vedrà il suo ricorso respinto.

L' ARBITRATO

Il Regolamento prevede anche un vero e proprio arbitrato irrituale. Secondo l'originario progetto di regole che il Comitato esecutivo aveva proposto nel 1999 all'assemblea della Naming Authority, esso avrebbe dovuto essere obbligatorio per tutti coloro che avessero registrato un nome a dominio. In tal modo, esso avrebbe costituito il fulcro di un sistema che, nell'ambito del diritto privato, avrebbe dato ad Internet non solo l'autonomia normativa, ma anche quella giurisdizionale, creando un sistema analogo a quello su cui si regge l'autonomia degli ordinamenti sportivi.

Miopi interessi di carattere sostanzialmente commerciale bocciarono l'arbitrato obbligatorio, che se da un lato sarebbe stato un ostacolo ben più serio delle procedure di riassegnazione all'accaparramento dei nomi a dominio (accaparramento che puntualmente si sarebbe verificato con la liberalizzazione del 1999), dall'altro era l'unico mezzo per garantire una vera autonomia del sistema, che oggi sconta la cronica lentezza e, a volte, l'inadeguatezza tecnica della magistratura ordinaria nel risolvere le controversie nascenti nel mondo di Internet.

L'arbitrato è comunque rimasto, seppur facoltativo, come uno dei mezzi previsti dal regolamento per la risoluzione delle dispute fra privati relative all'assegnazione dei nomi a dominio. Presso il Registro è tenuto un elenco di arbitri accreditati, erede del precedente comitato di arbitrazione della Naming Authority; il che dovrebbe garantire gli utenti della competenza degli arbitri stessi. Il procedimento è disciplinato dal regolamento in modo piuttosto snello, nel rispetto del contraddittorio, con termini alle parti per le difese. Il collegio arbitrale è di tre membri, nominati uno ciascuno dalle due parti ed il terzo d'accordo fra i primi due o, in mancanza di accordo, dal Registro. Il lodo deve essere pronunciato entro 90 giorni dalla costituzione del collegio ed è inappellabile.

Una interessante peculiarità di questo procedimento arbitrale sono i poteri cautelari concessi al collegio in relazione al nome a dominio in contestazione. I provvedimenti cautelari presi dal collegio su richiesta di una della parti (p.es.: sospensione del dominio) sono immediatamente eseguiti dal Registro.

Nonostante la buona fattura delle relative norme, l'arbitrato non ha avuto ad oggi molto successo, verosimilmente per il fatto che esso - al contrario delle procedure di riassegnazione - richiede per il suo esperimento il preventivo consenso esplicito di entrambe le parti. Non è quindi uno strumento

per la lotta al cyberquatting, come essenzialmente sono le procedure di riassegnazione, ma un vero e proprio mezzo per la risoluzione delle dispute alternativo al ricorso alla magistratura.

Per queste sue caratteristiche, qualora fosse posto come obbligatorio a chiunque registri un nome a dominio in Italia, sarebbe in grado di rendere autonomo il sistema dei nomi a dominio italiano; come in effetti è autonomo il sistema dei domini .eu, nel quale le procedure di riassegnazione sono in realtà dei veri e propri arbitrati, in quanto previsti esplicitamente dal regolamento della Commissione dell'Unione europea n. 874/2004 del 28 aprile 2004.

LA TUTELA DELL'UTENTE NEI CONFRONTI DEL REGISTRO

Tanto il Regolamento è diffuso e specifico nel predisporre mezzi volti a risolvere le questioni relative a nomi a dominio fra gli utenti quanto è carente e latitante nel fornire tutela all'utente nei confronti dei maintainer e del Registro stesso.

Non solo infatti non è previsto alcun tipo di procedura con la quale l'utente possa risolvere proprie controversie con il Registro o i maintainer; ma tutto il sistema della registrazione dei nomi a dominio italiani è strutturato in modo tale che l'assegnatario del nome a dominio non abbia un rapporto contrattuale diretto con il Registro, e non possa quindi vantare alcun diritto nei confronti del Registro. Sotto il profilo giuridico, infatti, il sistema dei nomi a dominio italiano è incentrato sul rapporto Registro - maintainer.

Solo fra essi intercorre un rapporto contrattuale (il cosiddetto "contratto maintainer") e solo nei confronti di questi ultimi il Registro assume obbligazioni contrattuali in relazione all'assegnazione e alla gestione dei domini. Il contratto maintainer è un contratto a prestazioni corrispettive di durata biennale, redatto su testo uniforme imposto dal Registro, nel quale il Registro sostanzialmente assume l'obbligazione di registrare e mantenere i nomi a dominio che gli sono richiesti dal maintainer secondo quanto previsto dal regolamento, mentre il maintainer è tenuto a pagare il corrispettivo pattuito per ciascun nome a dominio.

Nessuna obbligazione contrattuale assume invece il Registro nei confronti dell'assegnatario del nome a dominio, che pure è il diretto interessato e colui che, in definitiva, sostiene il costo della registrazione. Il Regolamento prevede infatti una serie di obblighi dell'assegnatario, di cui è responsabile nei confronti del Registro il maintainer, quale controparte contrattuale; ma nessuna obbligazione diretta è prevista a carico del Registro nei confronti dell'assegnatario.

Quest'ultimo, per registrare un nome a dominio, è tenuto necessariamente a passare per un maintainer e a sottoscrivere una "lettera di assunzione di responsabilità" che è in sostanza un vero e proprio atto di sottomissione. In essa l'assegnatario si assume tutte le responsabilità che derivano dall'utilizzo e dalla gestione del nome a dominio di cui chiede l'assegnazione; ma nessuna obbligazione contrattuale il Registro assume nei suoi confronti.

Né il contratto maintainer può ritenersi un contratto a favore di terzi, in quanto, al di là della pur necessaria indicazione contrattuale in tal senso, ciò è escluso a priori dal suo contenuto e dalla sua struttura, nella quale le obbligazioni delle parti sono riferite ad un numero indefinito di domini e le relative obbligazioni non eseguibili se non rispettivamente dal Registro e dal maintainer. In siffatta situazione l'utente assegnatario, che pure è colui che sostiene il costo della registrazione e si assume la responsabilità del dominio, è privo di autonoma, concreta tutela nei confronti del Registro.

Unico legittimato a far valere violazioni del Regolamento (che costituisce parte integrante del contratto maintainer e quindi la fonte delle obbligazioni contrattuali reciproche di Registro e maintainer) è il maintainer; sicché, di fatto, l'utente è tutelato se ed in quanto il suo maintainer ritenga opportuno ed abbia interesse a far valere egli stesso le eventuali violazioni del regolamento poste in essere dal Registro nella registrazione o nella gestione di quel singolo specifico nome a dominio.

È ovvio che, in concreto un tale interesse da parte del maintainer non si rinviene mai. Un maintainer che registra migliaia e migliaia di nomi a dominio versando al Registro un corrispettivo unitario di 4,91 euro iva esclusa non ha alcun interesse a iniziare per conto di un singolo cliente o per un singolo nome a dominio un contenzioso con il Registro stesso. L'utente rimane pertanto privo di alcuna tutela nei confronti del Registro.

E mentre per quanto riguarda il rapporto con il maintainer l'utente può almeno scegliere quello, fra le centinaia presenti sul mercato, che gli offra condizioni contrattuali che meglio lo garantiscano, nei confronti del Registro non può compiere scelta alcuna, non solo perché il Registro agisce, per motivi di carattere tecnico, in regime di monopolio di fatto, ma soprattutto perché esso comunque non stipula alcun contratto diretto con gli utenti, da cui pure trae gli oltre 6 milioni e mezzo di euro versatigli ogni anno per la registrazione e il mantenimento dei nomi a dominio.it.

L'utente è quindi privo di qualsiasi tutela nei confronti del Registro, al quale, non essendovi per l'appunto contratto alcuno, non possono neppure applicarsi le norme del Codice del consumo sul contratto del consumatore.

È quindi auspicabile che nel contesto dell'attuale rinnovamento programmatico e gestionale del Registro, in corso attualmente con la redazione da parte della Commissione per le Regole del nuovo sistema sincrono di registrazione dei domini, i rapporti fra utente, registro e maintainer (in futuro anche registrar) siano esattamente qualificati anche sotto il profilo giuridico, identificando esattamente gli istituti contrattuali e precisando per ciascuno il proprio ruolo ed i reciproci diritti e doveri.

ANDREA MAGGIPINTO

Internet e pubbliche amministrazioni: quale democrazia elettronica?

Andrea Maggipinto, Dottorando di ricerca in Informatica Giuridica e Diritto dell'Informatica presso il Centro Interdipartimentale di Ricerca in Storia del Diritto, Filosofia e Sociologia del Diritto e Informatica Giuridica (C.I.R.S.F.I.D. - Università di Bologna). Avvocato e Direttore dell'Osservatorio "Centro Studi di Informatica Giuridica di Milano", associazione no profit che opera per lo sviluppo della cultura e della conoscenza del diritto applicato alle nuove tecnologie. È Autore di articoli e volumi sugli aspetti giuridici dell'Information and Communication Technology e componente dei direttivi delle riviste "Diritto d'Autore e Nuove Tecnologie" e "Rivista di Diritto, Economia e Gestione delle Nuove Tecnologie". Si occupa scientificamente di e-government e cooperazione tra Pubbliche Amministrazioni.

PREMESSA

Il "governo elettronico" - c.d. e-government o electronic government - è fenomeno complesso e multidimensionale. Questo intervento non esaurisce tutti gli aspetti della rivoluzione elettronica in ambito pubblico, ma si pone l'obiettivo di individuare i livelli strategici di interazione tra cittadini, amministrazioni territoriali e organi di governo, portando all'attenzione del lettore taluni punti critici del percorso intrapreso nel nostro Paese dai piani di e-government e proponendo, per ciascuno di essi, alcune riflessioni.

Nello spirito che accomuna gli studiosi di Internet, le considerazioni qui formulate attendono argomentazioni critiche, perchè il futuro della Rete e della "società interconnessa" risiede essenzialmente nella dialettica e nel libero confronto di idee.

AMBITO DI INDAGINE: IL DIALOGO TELEMATICO TRA AGENTI

Non di rado il processo di ammodernamento degli enti e degli organismi pubblici viene inteso, semplicisticamente, come il risultato dell'introduzione nella pubblica amministrazione (PA) di applicazioni informatiche e tecnologie digitali per lo svolgimento delle funzioni istituzionali ad essa affidate.

La scienza informatica e le nuove applicazioni tecnologiche basate sull'elaborazione automatica dell'informazione, in realtà, hanno avviato un progressivo mutamento della sensibilità individuale e della cultura sociale che ha evidentemente interessato anche il settore pubblico e i rapporti giuridici

con le Istituzioni. Nuovi strumenti e nuovi obiettivi sono emersi da questo pulsante brodo tecnologico, generatosi peraltro in un momento storico nel quale la pubblica amministrazione aveva (da poco) avviato un processo di modernizzazione organizzativa e procedurale con le Leggi nn. 142 e 241 del 1990.

La retroazione amplificatrice determinata dall'informatica e dalla telematica - che stenta a definire con chiarezza quale evoluzione stia apportando al diritto pubblico - tanto rileva in quanto realizzi l'obiettivo primario del processo di ammodernamento: attuare quei principi e quei valori che fondano un moderno Stato democratico (semplificazione, trasparenza e perequazione sociale).

Le nuove tecnologie sono il risultato dell'applicazione delle conoscenze acquisite nell'ambito della scienza informatica a modi di procedere rivolti a scopi pratici. Nel settore pubblico questi "scopi pratici" sono propri della funzione pubblica e dell'interesse collettivo. Qui, dunque, la missione del progresso tecnologico si connota per le grandi aspettative che gli utenti ripongono nell'innovazione, ma anche per le grandi responsabilità di chi è oggi demandato a governarne la realizzazione.

Come in ogni segmento dell'organizzazione sociale, la rivoluzione digitale in ambito pubblico poggia su quella che ormai comunemente viene chiamata "Information and Communication Technology" (ICT), ossia la tecnologia dell'informazione e della comunicazione. In questo vorticoso mutamento di mezzi e di obiettivi, il dialogo telematico tra agenti - pubbliche amministrazioni (PPAA), cittadini e imprese - rappresenta la chiave di volta per lo sviluppo dei piani di e-government.

Attraverso la comunicazione interattiva e l'accesso alle informazioni si può infatti realizzare quella condivisione della conoscenza che, nei rapporti tra cittadini e organi di governo, rappresenta al contempo strumento e obiettivo primario del settore pubblico. In questa evoluzione digitale della società, avviata da poco più di un decennio, anche la relazione tra cittadino e pubblica amministrazione è destinata a mutare.

TRE LIVELLI DI COMUNICAZIONE ELETTRONICA

A differenza di altri settori, come quello del commercio elettronico per esempio, in Italia la pubblica amministrazione - in quanto destinataria principale della legislazione in materia di innovazione tecnologica (si pensi alla Legge 59/1997 e, da ultimo, al CAD, il "Codice dell'amministrazione digitale" approvato con D.Lgs. 82/2005) - ha potuto maturare una maggiore

esperienza nell'impiego delle ICTs. Regole ben definite hanno, infatti, permesso alle amministrazioni di procedere più celermente nell'implementazione delle tecnologie di gestione e trattamento dell'informazione elettronica. L'information technology rappresenta, dunque, l'ambito di maggiore sviluppo dei piani di e-government (si pensi, ad esempio, alla protocollazione e alla gestione documentale).

È invece la "comunicazione elettronica" a rappresentare oggi la vera sfida per il settore pubblico. Le amministrazioni italiane trovano ancora ostacoli e difficoltà lungo questo percorso di sviluppo dell'innovazione, perchè tradizionalmente non abituate al confronto con realtà esterne alle proprie competenze territoriali. Benché strettamente connesso alla tecnologia per il trattamento dell'informazione elettronica, è dunque quello della "communication technology" l'ambito dal quale dipenderà lo sviluppo del processo di ammodernamento delle PPAA.

Tre, in particolare, sono i livelli nei quali si possono articolare e sviluppare le nuove forme di comunicazione: livello inter-amministrativo (dialogo tra PPAA); livello inter-soggettivo (dialogo cittadino-PA); livello politico-istituzionale (dialogo Cittadini-Istituzioni).

Fruibilità dei dati e cooperazione applicativa (primo livello)

Nella Società dell'Informazione ogni atto, fatto o dato si trova ad essere oggetto di un fenomeno tipico dell'era tecnologica: la disgregazione informativa. I rischi che corrono le pubbliche amministrazioni in questa prima fase di digitalizzazione delle informazioni sono essenzialmente due: da un lato, la proliferazione di informazioni inerenti un determinato fenomeno, la cui scomposizione analitica porta ogni indagine da aggregati di informazioni strutturate a nuclei informativi più dettagliati, spesso decontestualizzati e perciò stesso privi del significato e della capacità semantica originari; dall'altro lato, l'applicazione puerile e immatura dell'informatica, tale da non rendere possibile il pieno controllo ed una esaustiva conoscenza delle vicende riferite a ciascun nucleo informativo.

Nel settore pubblico, la difficoltà di gestione dei dati è particolarmente elevata, stante la mole di informazioni gestite. La necessità di una funzione pubblica efficiente è quanto più importante tanto più se si pensa alle finalità istituzionali dei soggetti pubblici, i quali sono chiamati a dialogare tra loro scambiandosi, quando possibile (tecnicamente e giuridicamente), le informazioni in loro possesso, ottimizzando e migliorando i servizi resi ai cittadini e alle imprese. Le informazioni

contenute nelle banche dati diventano uno strumento essenziale e rappresentano un importante valore sia per le Amministrazioni, sia per gli utenti finali.

Gestire in modo ottimale ed organico le informazioni nell'ambito dell'intero sistema pubblico - identificando in modo specifico ed univoco, ad esempio, il luogo in cui l'informazione nasce e viene trattata, in funzione delle diverse competenze istituzionali - pare strategicamente importante. Altrettanto rilevante è la concreta ed effettiva possibilità che queste informazioni siano rese immediatamente disponibili, in modo efficace ed efficiente, a tutti i soggetti che ne necessitano per lo svolgimento delle loro attività.

Le pubbliche amministrazioni sono chiamate ad organizzare il proprio patrimonio informativo in considerazione del loro inserimento in un macro sistema. Si trovano, dunque, ad affrontare problematiche che superano la mera gestione interna del singolo dato. Nel governare l'innovazione di un sistema così complesso è, dunque, necessario mantenere una visione generale, che non si limiti a considerare le esigenze delle singole amministrazioni, ma che abbracci le questioni fondamentali dell'intero sistema. La fruibilità dei dati - ovvero la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione - rappresenta un obiettivo strategico, oltre che una strada obbligata per conseguire livelli accettabili nella qualità dei dati e dei servizi delle pubbliche amministrazioni.

Qualità ed efficienza sono condizioni essenziali e irrinunciabili per un reale ammodernamento del settore pubblico. Perchè i dati siano realmente "fruibili" e il sistema pubblico sia davvero efficiente, è necessario realizzare l'automazione dei processi di interazione tra pubbliche amministrazioni, ciò che si definisce "cooperazione applicativa". Questa nozione sta ad indicare l'insieme dei metodi e delle tecnologie in grado di realizzare una effettiva condivisione di dati, informazioni e processi tra due o più amministrazioni. Per poter realizzare un'efficace rete di cooperazione è indispensabile che le PPAA adottino standard comuni, sia a livello fisico (la rete telematica che permette fisicamente la trasmissione dei dati) sia a livello logico (grammatica e semantica di comunicazione).

Ad oggi, il livello fisico della rete di interconnessione tra PPAA è idoneo a realizzare una effettiva circolazione dei dati e delle informazioni. Con il D.Lgs. 28 febbraio 2005 n. 42 è stato istituito il Sistema Pubblico di Connettività (SPC), l'infrastruttura tecnologica per lo scambio di informazioni tra pubbliche amministrazioni, che persegue la finalità di assicurare il coordinamento informativo e informatico tra PPAA centrali e locali, nonché di promuovere l'omogeneità dell'elaborazione e

trasmissione dei dati. Il SPC - la cui disciplina è oggi inserita nel D.Lgs. 82/2005 - rappresenta dunque il quadro tecnologico di riferimento per la cooperazione e lo scambio delle informazioni tra le diverse amministrazioni.

Ogni amministrazione che intende affacciarsi sulla rete nazionale deve costituire un dominio, definito come l'insieme delle proprie risorse hardware, software e di comunicazione. Il dominio rappresenta il confine di responsabilità di un Ente, delle politiche che definiscono il suo sistema informativo. Per consentire l'interfacciamento tra un dominio e il resto della rete nazionale, è necessario un meccanismo di astrazione, chiamato "porta di dominio". Quest'ultima rappresenta l'unico punto di contatto telematico tra domini appartenenti a diverse PPAA ed effettua l'instradamento, a livello applicativo, dei messaggi in ingresso e in uscita dal dominio.

La porta di dominio rappresenta un elemento di disaccoppiamento: verso l'esterno tutti i domini devono omologarsi agli standard previsti dalla rete nazionale; al suo interno ogni dominio può conservare la propria struttura e le proprie scelte tecnologiche, lasciando alla porta di dominio la funzione di adattatore tra i due ambienti. Si ricordi infatti che, allo stato attuale, i sistemi impiegati dalle varie PPAA sono caratterizzati da una forte eterogeneità: diversi ambienti operativi, linguaggi di programmazione, politiche di sicurezza, e così via.

Gli attuali progetti di e-government non incontrano particolari difficoltà di cooperazione quanto al livello fisico. Piuttosto il vero problema - e la sfida dei prossimi anni - è rappresentato dal livello "logico", in particolare da quello semantico che si occupa della definizione e della gestione concettuale delle informazioni che i domini devono scambiarsi per poter raggiungere un determinato obiettivo. Le singole amministrazioni, nello svolgere funzioni e compiti omogenei, adottano procedure interne proprie, definite dai rispettivi regolamenti comunali che possono disciplinare in modo differente determinati servizi e procedure.

Per l'erogazione di un servizio o per lo svolgimento di un'attività, talune amministrazioni possono dunque richiedere e trattare informazioni in modo diverso rispetto ad altre PPAA, di modo che risulti difficile definire una semantica omogenea in grado di realizzare il dialogo telematico inter-amministrativo. Gli attuali piani di e-government, dunque, devono affrontare questo tema per individuare una soluzione che risulterà essenziale per il successo dell'intero processo di modernizzazione del Paese. Obiettivo primario dovrà dunque essere la realizzazione della cooperazione applicativa tra amministrazioni attraverso l'individuazione (i) di standard per la

rappresentazione e la codifica dei dati e delle informazioni e (ii) di standard di processo e interazione tra PPAA.

Questa "standardizzazione dei processi" interni alle PPAA avrà un grande impatto sul futuro del settore pubblico, in quanto consentirà di avere una gestione uniforme dei processi interni alle amministrazioni e permetterà di realizzare delle sovrastrutture di interazione realmente funzionanti. Ai profili strettamente tecnologici si affiancano, dunque, aspetti di natura logico-giuridica e organizzativa.

Un ruolo decisivo potrà essere svolto da "modelli di cooperazione" in grado di coordinare soggetti aventi distinte e diverse competenze. Si può ad esempio immaginare un "modello comunale" condiviso da tutti gli Enti, che non dovrà limitarsi all'insieme di servizi minimi che devono essere erogati, ma dovrà spingersi verso la definizione di interfacce applicative che permettano ai sottosistemi informatici dell'ente di parlare tra loro e con quelli di altri soggetti pubblici.

La definizione di standard normativo-regolativi sarà certo foriera di difficoltà. Non è infatti immaginabile che le amministrazioni locali si adeguino passivamente a standard definiti a livello nazionale. Altrettanto vero è, per contro, che senza modelli di processo condivisi si rischia il fallimento dei progetti di e-government. Una nota positiva giunge dall'esperienza di questi ultimi anni: gli stessi Enti locali richiedono l'applicazione di standard condivisi. È quindi plausibile ipotizzare che si possa realizzare una "cooperazione dal basso", ma questo processo deve essere favorito, guidato e soprattutto coordinato.

È indispensabile individuare metodologie di cooperazione tra le pubbliche amministrazioni anche in fase di definizione delle informazioni e delle funzionalità che devono essere scambiate tra loro, nonché di progettazione di software cooperativi, in grado di mettere a disposizione di altri applicativi le proprie funzionalità, per esempio attraverso architetture multi-layer e processi di workflow. Da questo scenario emerge la necessità di realizzare, per il futuro stesso dei piani di e-government e per l'ammodernamento del settore pubblico, un coordinamento equiordinato tra amministrazioni territoriali e amministrazione centrale. Il processo sarà evidentemente complesso.

Per evitare la differenziazione del settore pubblico in sottosistemi parziali e non interoperabili, una prima via percorribile può essere rappresentata dall'avvio di un coordinamento a livello regionale, nel quale ogni Ente locale possa partecipare ad un network paritario coordinato dalla Regione. In

questo modo si garantirebbe un continuo dialogo tra enti locali ed una sufficiente uniformità nei processi interni, talché i dati e le informazioni detenute da una amministrazione siano realmente disponibili ed accessibili per via telematica alle altre amministrazioni.

Il coordinamento nazionale per la modellazione dei procedimenti intra ed inter amministrativi - indipendenti dalle tecnologie - può essere garantito dall'apporto della Conferenza Unificata Stato-Regioni-Città e Autonomie locali, che in questa veste rappresenta il luogo ideale per la guida del Paese verso la realizzazione della cittadinanza digitale.

Accesso telematico a dati e documenti (secondo livello)

È chiaro che il percorso tracciato dalla legislazione degli ultimi anni segna un importante momento di evoluzione anche nei rapporti tra cittadini e pubbliche amministrazioni. Va in particolare ricordata la Legge 15/2005, che, accogliendo gli orientamenti prevalenti in dottrina e giurisprudenza, ha novellato la legge sull'accesso delineando una disciplina puntuale e precisa, ancorché siano state sollevate perplessità sull'efficienza della procedura prevista. Il nuovo articolo 22 della Legge 241/1990 attribuisce il diritto d'accesso a tutti i privati portatori di un interesse diretto, concreto ed attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento per il quale è richiesto l'accesso.

È irrilevante che il documento sia stato formato dall'amministrazione destinataria della richiesta di accesso. Gli elementi qualificanti sono la detenzione da parte dell'amministrazione e il fatto che il documento concerni un'attività non più semplicemente amministrativa, ma di interesse pubblico. In un contesto tecnologico, di informatizzazione delle procedure di accesso, la norma richiamata pone un problema di non poco momento. Essa, infatti, stabilisce la "non accessibilità" delle informazioni che non abbiano forma di documento amministrativo. Così prescrivendo, tuttavia, si trascura la nozione di documento informatico adottata nel nostro ordinamento [1], che abbraccia, al pari della rappresentazione di atti o fatti, anche la rappresentazione di dati.

L'accesso telematico, dunque, dovrebbe tener conto di questo aspetto importante: nell'era di Internet e della comunicazione digitale deve essere garantito l'accesso anche ai dati che abbiano una rilevanza autonoma e giuridica, altrimenti si rischierebbe di limitare le potenzialità delle innovazioni tecnologiche in ambito pubblico. Tuttavia, quanto stabilito dal nuovo art. 22 della legge 241/1990 non sembra essere il risultato di una scelta pienamente consapevole, piuttosto il prodotto della difficoltà di governare in modo coerente l'innovazione del settore pubblico nel suo complesso.

Basti considerare che sia l'art. 59 del D.P.R 445/2000 sia l'art. 52 del D.Lgs. 82/2005 riconoscono l'importanza dell'accesso per via telematica ai dati e alle informazioni delle PPAA, e non solo ai documenti amministrativi. È dunque necessario che, attraverso la reingegnerizzazione dei processi interni alle amministrazioni, sia garantita anche la disponibilità dei dati digitali detenuti dalla PA nei propri registri e archivi. La complessità del processo di ammodernamento del settore pubblico emerge ancor più chiaramente se si considerano le interrelazioni esistenti tra i primi due livelli di comunicazione (inter-amministrativo e inter-soggettivo).

Anche nei rapporti tra cittadino e amministrazione, infatti, risulta determinante il coordinamento e la cooperazione tra PPAA, al fine di individuare regole operative sull'accesso che siano in grado di garantire uniformità a livello nazionale. Solo una cooperazione applicativa integrata alle procedure di accesso telematico potrà realizzare quell'importante obiettivo fissato dal piano di e-government del 23 giugno 2000: "il cittadino potrà ottenere ogni servizio pubblico, cui ha titolo, rivolgendosi ad una qualsiasi amministrazione di front-office abilitata al servizio, indipendentemente da ogni vincolo di competenza territoriale o di residenza".

Non si deve dimenticare, infatti, la rilevanza dei servizi pubblici erogati telematicamente. Essi rientrano tra le finalità strategiche delle politiche di ammodernamento del settore pubblico, sia a livello comunitario, sia a livello nazionale: rappresentano uno dei passaggi centrali dei piani di e-government [2].

Ciò nonostante, si sceglie in questa sede di non affrontare questo tema per due ordini di ragioni: in primo luogo, perchè i servizi on line sono oggetto di ampia trattazione da parte della letteratura, ancorché non sempre con la giusta attenzione quanto alle precondizioni di back-office necessarie per la completa gestione dei servizi telematici avanzati; in secondo luogo, per evidenziare che, in questa fase del processo di ammodernamento pubblico, altri grandi temi necessitano di rinnovato impegno.

Un'ampia transizione verso modalità di erogazione on line dei servizi pubblici potrà infatti realizzarsi solamente attraverso una coerente progettazione dei processi di back-office e un effettivo dialogo telematico tra sistemi informativi (i.e. interoperabilità evoluta e cooperazione applicativa). Oggi, una disposizione programmatica contenuta nel D.Lgs. 82/2005 sembra individuare la via per il futuro dell'amministrazione digitale: "Le pubbliche amministrazioni collaborano per integrare i

procedimenti di rispettiva competenza al fine di agevolare gli adempimenti di cittadini ed imprese e rendere più efficienti i procedimenti che interessano più amministrazioni, attraverso idonei sistemi di cooperazione" (art. 63 comma 3 CAD).

Partecipazione e trasparenza (terzo livello)

Le tecnologie di comunicazione rilevano direttamente nei rapporti tra Cittadini e Istituzioni, sia che si ritenga persista il "principio di divisione" tra Stato e società civile, sia che si aderisca alla posizione di chi vede, nello sviluppo dei diritti sociali, una maggiore, e tendenzialmente perfetta, corrispondenza tra governanti e governati. Non di rado con l'espressione "democrazia elettronica" (o e-democracy) si individuano nuove forme e modalità di partecipazione diretta dei cittadini alla vita politica. Invero, questa espressione evoca tensioni e valori più ampi e universali.

Non è possibile individuare un modello unico di governo democratico. Molteplici le ragioni (soprattutto extra-giuridiche) che determinano la scelta verso una particolare forma di stato e di governo, e queste ragioni non possono essere certamente condizionate dall'introduzione delle nuove tecnologie. Esse, piuttosto, possono coadiuvare le Istituzioni nel realizzare e gestire in modo più efficiente i meccanismi e le procedure alla base del funzionamento dello Stato, siano essi strumenti di democrazia diretta, deliberativa o rappresentativa. La governance dell'innovazione tecnologica rappresenta una via per alimentare il continuo rinnovamento verso modelli sempre più efficienti.

Non vanno in ogni caso sottovalutate le forme di partecipazione dei cittadini alla vita pubblica. La collaborazione tra cittadini e amministrazione è certamente un aspetto positivo, se ben progettata e costruita. Due, tuttavia, possono essere le ragioni per le quali gli strumenti di partecipazione diretta non rappresentano il nodo centrale dell'innovazione tecnologica nella società contemporanea. In primo luogo, nelle c.d. democrazie avanzate pare emergere piuttosto chiaramente che l'ampiezza e la sicurezza della sfera dei diritti riconosciuti ai cittadini tendono ad assopire il coinvolgimento dei cittadini nella vita politica, quasi favorendo un atteggiamento passivo, di disinteressamento verso le attività svolte dalle Istituzioni.

Ciò, al contrario, sembra essere il motivo dell'importanza riconosciuta dalla politica agli strumenti di democrazia diretta nei Paesi in via di sviluppo. In secondo luogo, vanno considerati i reali ostacoli alla partecipazione attiva dei cittadini nelle fasi decisionali e nei processi di formazione delle leggi. Essi non sono certamente di natura tecnologica, ma organizzativa, culturale e financo costituzionale. Prima o contestualmente alla progettazione di strumenti tecnologici per la

partecipazione diretta dei cittadini alle fasi decisionali delle Istituzioni, sarebbe dunque opportuno prendere coscienza di quanto emerso dai numerosi studi condotti in ambito politico-sociale sulle difficoltà e i problemi posti dalla c.d. democrazia diretta.

Con ciò, si ribadisce, non si vuole negare l'importanza degli strumenti di partecipazione. Al contrario. Muovendo dalla tesi pluralista che evidenzia lo stato di crisi della democrazia rappresentativa, sembra ragionevole attendersi un maggiore coinvolgimento nella vita politica delle realtà associative e di gruppi di interesse. In definitiva, una valorizzazione di meccanismi assimilabili agli strumenti di democrazia deliberativa. La società tecnologica rende evidente un problema di fondo delle società democratiche: la necessità di ridurre la complessità dei problemi, affinché possano essere accessibili ai processi democratici. L'interdipendenza che caratterizza ogni settore della società acutizza la complessità delle decisioni politiche.

Più complesso diventa dominare i processi decisionali in modo coerente. In una realtà come quella odierna, tecnico-scientifica e altamente organizzata, deve essere affrontato il rischio di discrasia tra le competenze specifiche e le competenze decisionali, rischio che può portare a uno scollamento tra decisioni politiche ed esigenze sociali. Non è dunque un caso che si siano introdotti strumenti, come per esempio le consultazioni pubbliche, che mirano al coinvolgimento - seppur in modo non vincolante - delle realtà più organizzate del tessuto sociale. Questi sono strumenti che incentivano l'associazionismo e veicolano all'interno delle istituzioni il pensiero e le opinioni di comunità e realtà locali. Il progresso tecnologico è in grado di favorire questo coinvolgimento e, al contempo, ne rappresenta vivo presupposto.

Con riferimento ai piani di e-government, è necessario che gli organi di governo sappiano coordinare un piano decisionale coerente ed efficiente sulla base delle proprie capacità di governance, nonché grazie all'esperienza e alle competenze di coloro i quali - scienziati, studiosi e operatori del settore - siano in grado di apportare il know how e il know why indispensabili. Quanto agli strumenti di partecipazione, decisiva sarà la via per l'attuazione del principio generale sancito dall'art. 9 del Codice dell'amministrazione digitale: "Lo Stato favorisce ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili sia individuali che collettivi". La sfida per i decisori tecnologici si porrà nell'individuare forme idonee di partecipazione dei cittadini. Internet rappresenta un grande mezzo di condivisione e di incontro di idee; la funzione sociale della Rete delle reti è innegabile.

La partecipazione dei cittadini alla vita politica potrà dunque essere veicolata in primo luogo attraverso meccanismi, basati sui principi di libertà ed eguaglianza, che coinvolgano le comunità e i gruppi di azione. Questi meccanismi di "partecipazione strutturata" rappresentano un forte incentivo alla promozione e valorizzazione delle libere forme associative: significherebbe cogliere le istanze sociali e capire che le comunità, piccole o grandi, locali o globali, hanno la possibilità oggi, grazie a Internet, di realizzare momenti di discussione e cooperazione, anche politica. Questa forma di collaborazione organizzata risulterebbe utile per mantenere una posizione di mediazione tra la difesa degli interessi individuali, da un lato, e il potere politico decisionale riferito alla collettività, dall'altro. Questo, sia come metodologia democratica generale, sia per lo sviluppo dei piani di e-government.

L'efficienza funzionale delle istituzioni e delle pubbliche amministrazioni dipenderà da come verrà gestita questa mediazione, attraverso quali modelli e procedure di coordinamento e cooperazione. Il dialogo partecipativo e collaborativo tra Istituzioni e Cittadini potrà trovare giovamento nei nuovi mezzi di comunicazione e interazione elettronica. Sarà in ogni caso necessario che gli amministratori sappiano impiegare in modo opportuno questi strumenti e realizzare quelle precondizioni indispensabili per un'equa e distribuita partecipazione. Le reti civiche potrebbero essere rimodellate in community network, ossia reti a carattere partecipativo con forum e aree di discussione.

Tuttavia, la forza della Rete permette ai cittadini - senza l'intervento dei pubblici poteri - di costituire gruppi e comunità di discussione. I governanti, dunque, dovrebbero cogliere i segnali di una realtà ormai palesatasi, progettando e costruendo meccanismi democratici che sappiano valorizzare le opportunità che la tecnologica riconosce direttamente ad ogni singolo individuo. Al contempo i piani di e-government dovrebbero mirare a realizzare nel settore pubblico gli aspetti chiave della rivoluzione digitale: cooperazione interamministrativa, accesso alle informazioni, partecipazione strutturata. Nei rapporti tra Istituzioni e Cittadini vi è inoltre un altro aspetto da considerare, tutt'altro che irrilevante. Principio comune dei regimi democratici, il valore comune delle c.d. "società avanzate", è infatti la trasparenza dell'azione amministrativa e di governo (centrale o locale), ovvero la conoscenza/conoscibilità degli atti e delle attività delle Istituzioni. Internet rappresenta una grande risorsa per l'accesso alla conoscenza.

La possibilità - e il diritto - di accedere agli atti istituzionali, alle informazioni sulle attività di governo, e anche al patrimonio normativo e giuridico sui poteri e i compiti delle Istituzioni, sono i presupposti fondanti i meccanismi di controllo dei cittadini e la responsabilità dei governanti. Lo stesso piano nazionale per l'e-government e i processi locali di reingegnerizzazione e digitalizzazione dell'azione amministrativa devono soddisfare questa esigenza di trasparenza, in un quadro programmatorio che renda conoscibili gli obiettivi fissati, i criteri usati per la loro individuazione e i risultati raggiunti. Questo approccio alle tecnologie dell'informazione e della comunicazione può mutare la comune accezione riconosciuta all'espressione "democrazia elettronica", evocando in primis quel valore universale che risiede nella realizzazione di una trasparenza informatica dell'azione di governo e nell'accesso agli atti e alle informazioni.

STATO DI DIRITTO, TECNOLOGIE E PRECONDIZIONI DI DEMOCRAZIA

Il modello di "Stato di diritto" individua, attraverso le tecnologie di informazione e di comunicazione, nuove vie di sviluppo, ma anche nuove sfide da affrontare. É bene anzitutto partire dalla considerazione che questo modello teorico è costruito, tra gli altri, su questi imprescindibili elementi: eguaglianza e libertà dei cittadini. Come il diritto e gli ordinamenti giuridici possono realizzare questi obiettivi in una società altamente tecnologica? Il problema delle attuali democrazie, come del resto di quelle del periodo prettamente industriale, è determinato dal rischio di divergenza tra principi costituzionali universali e principi che regolano l'azione dei Governi. Il riconoscimento formale dei diritti dell'individuo non assicura infatti un coerente esercizio del potere politico-amministrativo.

È necessario superare quel compromesso determinato dall'utilità sociale e dalla necessità politica, che genera un progressivo sbiadimento dei diritti individuali. Affinché il principio di uguaglianza possa trovare attuazione nella "società dell'informazione", devono essere garantite eguali condizioni di accesso all'informazione. I governi sono in primo luogo chiamati a realizzare quelle precondizioni presupposte all'autodeterminazione del cittadino, per evitare una altrimenti inevitabile frattura sociale (generazionale o territoriale). Invero, la frattura tra ricchi e poveri ha ulteriori e profonde radici. L'accesso all'informazione rappresenta una, non certo la sola, condizione per l'eguaglianza dei cittadini nel libero esercizio dei diritti politici e civili.

È in ogni caso compito delle Istituzioni quello di assicurare la formazione e l'alfabetizzazione informatica dei cittadini e dei dipendenti pubblici (si vedano gli articoli 8 e 13 del CAD) [3], fattori indispensabili per l'impiego delle nuove tecnologie nei rapporti con le pubbliche amministrazioni. I

governi devono assicurare, anche attraverso un sistema scolastico evoluto, un livello adeguato di conoscenza delle tecnologie, presupposto per la socializzazione e la formazione intellettuale e culturale dei cittadini. Vero è che l'alfabetizzazione informatica, senza la creazione di uno scenario nel quale sia davvero possibile utilizzare gli strumenti tecnologici, varrebbe a poco. Il c.d. "divario digitale" (o digital divide) rappresenta infatti la disuguaglianza dei cittadini sia nelle capacità di utilizzo delle nuove tecnologie, sia nelle condizioni di accesso ad esse.

Se le nuove tecnologie hanno un forte impatto sulla struttura ordinativa della società, e di essa creano le condizioni di emancipazione strutturale, il divario digitale, al contrario, frustra gli elementi caratterizzanti lo Stato di diritto, impedendo qualunque percorso di sviluppo democratico. Perchè in una società tecnologicamente avanzata si realizzi una "vera cittadinanza", devono dunque trovare attuazione tutte le precondizioni sociali e culturali. Realizzate queste precondizioni di democrazia, la richiesta di interazione telematica da parte dei cittadini, da un lato, e la capacità delle PPAA di soddisfare quelle richieste, dall'altro, innescheranno un processo virtuoso che progressivamente porterà alla completa digitalizzazione del settore pubblico.

È chiaro che la strada da intraprendere deve essere tecnologicamente neutrale e non può condurre a una specifica tecno-dipendenza. L'idea moderna di Stato di diritto - sotto la spinta multidimensionale delle tecnologie dell'informazione e della comunicazione - fa proprio l'obiettivo di governare il processo di democratizzazione sociale in atto. Non deve ergersi a decisore del bene comune, ma deve interpretare le istanze che emergono dall'uso sociale di Internet e dalle comunità virtuali che in ogni campo, in ogni settore, nascono e crescono. Bene, dunque, che lo Stato favorisca l'alfabetizzazione informatica, senza intraprendere strade a senso unico verso una particolare opzione tecnologica e fornendo ai cittadini gli strumenti per accedere alle risorse software e hardware rese disponibili dal progresso. La tecnologia non è un'entità autonoma che produce effetti e conseguenze sociali.

Nell'analisi dei rapporti tra società e tecnologia, è dunque necessario rivedere l'opinione di chi consideri quest'ultima come ragione dei cambiamenti sociali. In realtà, è vero anche l'esatto contrario: la società influenza la tecnologia e governa (o dovrebbe governare) il progresso tecnologico sulla base delle proprie esigenze. Come già emerso in altri ambiti (per esempio nel diritto ambientale e nella tutela del patrimonio naturale), anche con riferimento al progresso tecnologico e alle nuove esigenze di alfabetizzazione, lo Stato dovrebbe compiere scelte politiche che siano in grado di tutelare e salvaguardare i diritti dei cittadini di domani. I diritti delle future

generazioni dipenderanno anche dalle scelte che in questi anni si compiranno nel processo di ammodernamento degli Stati, in relazione ai diritti degli individui di fronte alle nuove tecnologie.

I sistemi di protezione sociale (c.d. Welfare State) possono realizzare diversi obiettivi, in relazione alla rilevanza e al peso riconosciuti all'equità sociale distribuita, all'efficienza o alla crescita economica. Tra i molti obiettivi vi è certamente la riduzione dell'esclusione sociale. Se si applicassero i criteri di indagine tipici delle trattazioni del diritto costituzionale e del diritto pubblico, ci si accorgerebbe che il processo di rinnovamento del settore pubblico attraverso modelli di e-government è poco più che in una fase iniziale. Chi sono i soggetti titolari dei diritti? Qual è il regime giuridico applicabile? Quali le forme di tutela dei diritti? Saremmo in grado di rispondere solo alla prima di queste domande, peraltro riservandoci su quanti effettivamente siano nelle indispensabili pre-condizioni di accesso e conoscenza. Il cammino dei piani di e-government - nel realizzare i tre livelli di comunicazione sopra descritti, tra loro strettamente collegati e interdipendenti - dovrà necessariamente giungere alla definizione di un regime giuridico sull'uso delle tecnologie in ambito pubblico che riconosca diritti realmente esigibili.

INTERNET E GLI STATI

L'attuale epoca è fortemente connotata dalle cause e dagli effetti del processo di globalizzazione. Tale processo è determinato essenzialmente da tre fattori: uno economico, ovvero lo sviluppo di traffici internazionali e di rapporti commerciali tra Stati; uno politico, sviluppatosi nel corso del XX secolo e determinato dall'abbattimento della cortina di ferro e della contrapposizione tra comunismo e capitalismo; uno, infine, tecnologico, che ha portato poco più di quindici anni fa alla nascita del World Wide Web. L'interconnessione globale rappresenta dunque una delle variabili del processo di mondializzazione in atto; esse determinano tra loro variazioni correlate, pur essendo reciprocamente indipendenti.

Dopo quasi un secolo dalla pubblicazione di "The Great Illusion", libro del premio nobel Norman Angell, sembra emergere in Internet una nuova interdipendenza tra gli Stati. Non è possibile sapere se e come si giungerà alla definizione di un diritto internazionale di Internet, una Rule of Cyberspace Law in grado di integrare culture di popoli diversi sulla base di valori e principi condivisi, imbrigliando così gli scatti di potenza dei Governi assoggettandoli al diritto. Certamente Internet ha e avrà un impatto determinante nei rapporti tra gli Stati. L'ideale di una democrazia elettronica si proietta sullo sfondo delle relazioni tra i popoli: la cooperazione dei Governi e delle comunità epistemiche risulta essenziale per la realizzazione di una governance transnazionale che

favorirà il riconoscimento, in ogni Nazione, dei fondamentali diritti del cittadino all'accesso all'informazione e alla conoscenza.

L'importanza di un diritto condiviso dell'Internet risiede non solo nel trovare regole sui rapporti giuridici instaurati per mezzo della Rete, ma anche e soprattutto sulle regole applicate ad essa. Queste regole governeranno Internet e condizioneranno le modalità di interazione tra individui e il processo stesso di emersione di un'universalità sociale. L'accesso all'informazione e alla Rete rappresenta un parametro importante con cui misurare il pensiero politico moderno. L'Europa ha un compito importante in questo processo internazionale di definizione della governance di Internet che non dovrà solo fondarsi sulla costruzione di mercati e relazioni commerciali, quanto su diritti, progetti e Istituzioni comuni.

La cultura politica europea, incentrata sull'uguaglianza e la libertà degli individui, può dunque rappresentare un importante contributo nel dibattito internazionale per valorizzare una concezione della tecnologia quale strumento per il miglioramento razionale delle società e delle Istituzioni. Positivo apprezzamento va alle iniziative del Governo italiano nell'intessere rapporti di cooperazione con altri Stati in tema di e-government. Con la realizzazione di modelli di governo elettronico nei Paesi in via di Sviluppo, l'Italia si propone di aumentare l'efficienza e la trasparenza dei processi democratici, favorendo le sinergie con altri Stati e, dunque, la crescita dei rapporti internazionali. Contribuire alla costruzione di modelli di governo elettronico significa favorire la circolazione e l'interscambio di informazioni a livello globale.

Le ragioni per le quali queste iniziative di collaborazione risultano particolarmente importanti sono essenzialmente due: (i) in primo luogo, l'Italia si fa parte attiva del progresso tecnologico in ambito internazionale e al contempo acquisisce capacità di realizzazione in contesti differenti, affinando le proprie capacità di governance; (ii) in secondo luogo, il nostro Paese favorisce la crescita (anche tecnologica) di Paesi in via di sviluppo, la cui presenta nel contesto mondiale è quanto mai importante per lo sviluppo di una visione condivisa di Internet. È nell'interesse di tutti che la comunità internazionale si popoli di nuove realtà di governo e nuove realtà sociali. In questo scenario di policentrismo internazionale, ciascuno Stato è chiamato a definire un proprio spazio politico che proietti su scala globale i diritti dell'uomo e del cittadino.
Se e come Internet modificherà le geometrie politiche degli Stati, dipenderà da come i Governi si sapranno relazionare sui grandi temi legati alla governance di Internet, e non solo. È ormai tempo che le Istituzioni nazionali e i governi sviluppino una politica tesa a ridefinire i processi tecnologici

realizzando modelli sostenibili, inclusivi e realmente efficaci per il riconoscimento dei diritti fondamentali dei cittadini. Il diritto pubblico, in questo contesto, può rappresentare la via per bilanciare - con razionalità globale - i rischi di un progresso tecnologico non sostenibile.

Così come le tecnologie di domani saranno il prodotto dell'evoluzione di quelle oggi esistenti, anche gli individui, come essere sociali, discenderanno da quelli delle generazioni che vivono questo tempo. I decisori hanno il compito di governare questa evoluzione - nella quale sistemi tecnologici e sistemi socioculturali amplificano l'uno il dominio d'azione dell'altro - favorendo il libero progresso tecnologico e garantendo eque condizioni di accesso alla conoscenza.

NOTE

[1] “La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti” (d.P.R. 445/2000 art. 1, c. 1, lett. b; CAD art. 1, c. 1, lett. p).

[2] Cfr.: Consiglio europeo di Lisbona, 23-24 marzo 2000; Decisione, Parlamento e Consiglio, 21 ottobre 2002, n. 2045/2002/CE; Comunicazione della Commissione del 1° giugno 2005 "i2010 - Una società europea dell'informazione per la crescita e l'occupazione"; Comunicazione della Commissione del 25.04.2006 COM(2006) 173 "Il piano d'azione eGovernment per l'iniziativa i2010: accelerare l'eGovernment in Europa a vantaggio di tutti". Inoltre: Piano nazionale di e-Government 22.06.2000; Direttiva M.I.T. del 4 gennaio 2005; Direttiva M.I.T.-M.F.P. 27 luglio 2005; D.Lgs. 7 marzo 2005, n. 82 (Sezione III - Capo IV); “Verso il Sistema nazionale di e-government” - Linee strategiche, marzo 2007.

[3] Art. 8 - Alfabetizzazione informatica dei cittadini: “Lo Stato promuove iniziative volte a favorire l'alfabetizzazione informatica dei cittadini con particolare riguardo alle categorie a rischio di esclusione, anche al fine di favorire l'utilizzo dei servizi telematici delle pubbliche amministrazioni”. Art. 13 - Formazione informatica dei dipendenti pubblici: “Le pubbliche amministrazioni nella predisposizione dei piani di cui all'articolo 7-bis, del decreto legislativo 30 marzo 2001, n. 165, e nell'ambito delle risorse finanziarie previste dai piani medesimi, attuano anche politiche di formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione”.

LAURENT MANDERIEUX

Internet e il diritto d'autore, una relazione necessaria ma tormentata

Laurent Manderieux, Adjunct Professore di Diritto della Proprietà Intellettuale, Università L. Bocconi, Milano, docente di proprietà intellettuale in numerosi corsi e programmi universitari e di formazione aziendale in Europa e nel Mondo; Esperto Senior presso diverse Organizzazioni Internazionali Organizzazione Mondiale della Proprietà Intellettuale (OMPI-Ginevra); United Nations Commission on International Trade Law (UNCITRAL, Vienna); International Development Law Organization (IDLO, Roma); Organisation Internationale de la Francophonie (OIF, Parigi ecc.), Amministratore Giurista alla FAO ed all,OMPI per 14 anni; le sue pubblicazioni più importanti riguardano il campo della proprietà intellettuale.

Internet e il diritto d'autore non possono vivere l'uno senza l'altro. In effetti, per il diritto d'autore, Internet rappresenta una sfida e un'opportunità di fondamentale importanza. Il diritto d'autore funziona sulla base di tre regole base:

la protezione sui generis, e automatica, vale a dire senza formalità;

la territorialità: il diritto viene concesso solo per il territorio di un paese e si estende ad altri Paesi nella misura in cui essi abbiano siglato tra loro un trattato di reciprocità;

la durata della protezione, uniforme per ogni categoria di opere e piuttosto lunga (da 50 anni in su).

Internet invece non è territoriale: qualsiasi ccTLD è accessibile da qualsiasi parte del mondo, i contenuti sono spesso di carattere effimero e le tecnologie che fanno funzionare Internet sono sempre costantemente migliorati e migliorabili. Lo sviluppo esponenziale di Internet non permette al diritto d'autore d'ignorare la centralità della rete nella creatività culturale e scientifica umana. D'altronde, il web ha una relazione strettissima con il tema del diritto d'autore: nei Paesi industrializzati gran parte dei contenuti messi online sono sottoposti alla tutela del diritto d'autore sotto una forma o un'altra (anche nel caso di diritto d'uso completamente libero), come anche l'architettura stessa di Internet, risultato del lavoro di migliaia di ricercatori e informatici, viene protetta o può essere protetta dal solo diritto d'autore. Inoltre, la rete si può sviluppare pienamente nella sua funzione commerciale solo per mezzo di un sistema di diritti creati legati in maniera molto stretta al diritto d'autore. Nella logica del presente Quaderno, questo contributo intende soffermarsi soprattutto sulla relazione d'Internet con il diritto d'autore, dando anche alla questione una necessaria dimensione Nord-Sud. Inoltre, nella logica degli altri contributi al Quaderno, il presente contributo si sofferma su Internet, diritto d'autore e gap Nord-Sud considerando essenzialmente la

questione del diritto d'autore per quanto riguarda i contenuti messi in rete: non si intende trattare in dettaglio il legame tra i sistemi che permettono alla rete di funzionare e il diritto d'autore; su quest'ultimo argomento numerosi articoli hanno analizzato, relativamente all'Europa, la complessa relazione triangolare tra software, diritto dei brevetti e diritto d'autore in occasione degli animati dibattiti che hanno preceduto il voto contrario da parte del Parlamento Europeo nel luglio 2005 al Progetto di Direttiva UE sulla brevettabilità delle invenzioni implementate tramite computer.

I TENTATIVI PER RENDERE PIÙ STABILE LA RELAZIONE INTERNET-DIRITTO D'AUTORE

L'interazione di Internet con il diritto d'autore rimane tuttora difficoltosa, poiché la rete ha di per sé un carattere internazionale e i siti di qualsiasi ccTLD o GTLD sono accessibili da qualsiasi computer in qualunque parte del globo, mentre il diritto d'autore rimane governato da ogni singolo Stato sul suo proprio territorio.

Il quadro normativo internazionale del diritto d'autore, che ha funzionato bene per un secolo, è quello della Convenzione di Berna per la protezione delle opere letterarie e artistiche, adottata nel 1886; è completato a livello nazionale da leggi d'applicazione. La Convenzione di Berna, capolavoro giuridico di semplicità ed efficacia ha potuto offrire delle risposte soddisfacenti in materia di diritto d'autore, con adattamenti di piccola entità, all'arrivo della radiodiffusione e della televisione. Invece, con l'arrivo di Internet la Convenzione si è rivelata desueta per la prima volta dalla sua creazione.

Già a partire dalla metà degli anni Ottanta si intuì quest'obsolescenza e la questione dell'aggiornamento della Convenzione di Berna venne indirettamente considerata nei negoziati che portarono nel 1994 alla creazione dell'Organizzazione Mondiale del Commercio (OMC), in particolare nei negoziati relativi alla conclusione dell'Accordo sugli aspetti dei diritti di proprietà intellettuale attinenti al commercio (meglio conosciuti come "Accordo TRIPS"), il capitolo dell'Accordo OMC relativo alla Proprietà intellettuale.

Tuttavia, è solo dagli anni Novanta che si percepisce la reale dimensione mondiale per Internet e poiché i trattati sono il frutto di negoziati lunghi, sarà attraverso due Trattati ulteriori agli Accordi TRIPs che sarà data una prima risposta all'obsolescenza della Convenzione di Berna e che saranno introdotti di conseguenza i tentativi di miglioramento della relazione tra Internet e il diritto d'autore: il WIPO Copyright Treaty (WCT) e il WIPO Performances and Phonograms Treaty (WPPT), più

comunemente chiamati "I Trattati Internet dell'OMPI" del dicembre 1996, resero più moderno il quadro generale del diritto d'autore della Convenzione di Berna in tre modi:

- tramite delle norme di diritto d'autore già sancite dai TRIPS;
- aggiornando alcune norme internazionali di diritto d'autore su questioni non specificamente legate alle tecnologie digitali;
- stabilendo, in particolare, nuove norme internazionali applicabili alle tecnologie digitali.

Nell'obiettivo di semplificare questo testo per rendere più agevole la comprensione ai lettori non addetti al lavoro giuridico, si può affermare a grandi linee che queste nuove norme rappresentano un chiarimento cruciale perché fanno entrare Internet e i contenuti messi on-line nella sfera delle opere protette dal diritto d'autore, ponendo fine ad ogni dubbio su questo fronte. Si nota che le nuove norme internazionali applicabili alle tecnologie digitali permettono in particolare l'istituzione, tramite le leggi nazionali di ratifica di questi Trattati, di misure dette di "antineutralizzazione" e di "protezione dell'informazione sul regime dei diritti", vale a dire di misure destinate a proibire i meccanismi destinati a neutralizzare i sistemi di autorizzazione dell'accesso ai contenuti digitali e all'uso non autorizzato di tali contenuti.

Gli Stati Uniti, l'Unione Europea e gli altri Paesi industrialmente sviluppati avevano fatto pressione per la rapida conclusione di tali Trattati, poiché intendevano permettere lo sviluppo dei sistemi DRM (Digital Right Management) o di sistemi software di gestione dei diritti che permettono il concretizzarsi di un regime legale per le opere on-line. E a dieci anni dalla conclusione di questi Trattati possiamo constatare che i loro ideatori hanno ottenuto gli effetti desiderati: gli Stati Uniti, con l'adozione del Digital Millenium Copyright Act (DMCA) nel 1998, e l'Unione Europea con l'attuazione, avvenuta in tempi lunghi, della Direttiva 2001/29 del maggio 2001 sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione (più comunemente chiamata Direttiva EU sul copyright o EUCD) e la ratifica di tutti i Paesi Membri, hanno confermato nelle loro leggi l'entrata dei contenuti su Internet nella sfera del diritto d'autore, e hanno così permesso lo sviluppo del commercio in rete di prodotti protetti dal diritto d'autore in rete o meno. In apparenza, la relazione di Internet con il diritto d'autore sembra dunque stabilizzata, almeno nei Paesi industrializzati.

DEI RISULTATI FRAMMENTATI

In realtà, la relazione di Internet con il diritto d'autore non è per niente stabilizzata, per almeno tre motivi principali:

- Il WIPO Copyright Treaty (WCT) e il WIPO Performances and Phonograms Treaty (WPPT) hanno permesso ai Paesi occidentali di elaborare dei testi giuridici (EUCD o DMCA) che da una parte favoriscono l'allargamento della proprietà privata su Internet (i cosiddetti modelli proprietari, sviluppati grazie ai DRM), dall'altra hanno suscitato una raffica di critiche di ordine etico, economico e sociale; in Occidente gli autori di queste critiche hanno sviluppato con qualche successo dei contro-modelli ai modelli proprietari, come è il caso di Creative Commons o di simili modelli di diritto d'autore, detti aperti. Questi modelli di diritto d'autore sono in realtà più à la carte che aperti poiché permettono al titolare di un'opera messa on-line - grazie al WIPO Copyright Treaty o al WIPO Performances and Phonograms Treaty si potrà trattare dunque di un'opera protetta dal diritto d'autore - di scegliere quale regime di protezione intende dare alla sua opera, usando uno o diversi modelli standard di "apertura" dei suoi diritti (diritto di riprodurre un'opera gratuitamente senza alterarla o con possibilità di alterarla unicamente per un uso non commerciale o permettendo l'alterazione, con o senza autorizzazione dell'autore, per uso anche commerciale). Questi modelli, nati spontaneamente come modelli "Bottom up" spesso grazie a stretti contatti dei loro ideatori con numerosi architetti della rete, sono perfettamente legali, o più esattamente si dovrebbe affermare che non sono per nulla contrari alle leggi varate (DMCA o EUCD), anche se tali testi sono stati ideati con una filosofia completamente diversa.

Inoltre, i modelli proprietari sono anche oggetto di una critica maggiore e ancora più radicale: nel campo scientifico, alcuni autori in Occidente, Italia inclusa, considerano che i modelli proprietari impediscono la ricerca scientifica poiché rallentano la diffusione della conoscenza; e di conseguenza questi autori considerano indispensabile riscrivere l'EUCD e il DMCA, interpretando i Trattati Internet dell'OMPI in un modo più neutro rispetto ai modelli proprietari.

- Si è dovuto prevedere, sia nel DMCA sia nel EUCD, delle eccezioni alle limitazioni del diritto d'autore per gli Internet Service Providers (ISP): queste eccezioni sono state rese necessarie dalla loro mera funzione di mezzi di transito dell'informazione. Si è anche dovuto prevedere delle eccezioni a favore delle Università, i cui studenti e alle volte docenti (il numero si può contare talvolta in migliaia di persone) possono violare dei diritti d'autore altrui usando i Siti Internet dell'Università.

- Infine e soprattutto, sono pochi i Paesi membri del WIPO Copyright Treaty e del WIPO Performances and Phonograms Treaty (una sessantina di Paesi in tutto, cioè un terzo dei Paesi del mondo) e questo ne impedisce l'efficacia, considerando che qualsiasi ccTLD o gTLD è accessibile da qualsiasi parte del mondo come già accennato, però anche che qualsiasi indirizzo Internet sotto qualsiasi ccTLD o gTLD può essere arricchito di contenuti tuttora chiaramente soggetti al diritto d'autore nei soli Paesi membri dal WCT e del WPPT.

Siamo dunque molto lontani da un sistema di diritto d'autore chiaro ed efficace per Internet. In particolare, diversi Paesi in sviluppo temono che il sistema stabilito dal WCT e dal WPPT sia sfavorevole ai loro interessi e contribuisca ad aggravare il divario Nord-Sud. I contenuti in rete di cui i Paesi del Sud del mondo necessitano per ridurre il proprio gap scientifico e tecnologico sono quasi sistematicamente realizzati nei Paesi del Nord del mondo.

Essi sono protetti (talvolta iperprotetti) dai Paesi del Nord grazie ai Trattati Internet dell'OMPI e a leggi di ratifica volutamente scritte per favorire i modelli proprietari. I governi dei Paesi del Sud, al fine di trovare un sostegno giuridico alla loro richiesta di accesso liberalizzato ad un numero maggiore di contenuti in rete, si riferiscono al primo paragrafo dell'Articolo 27 della Dichiarazione Universale dei Diritti Umani del 1948, che specifica:

"1. Ogni individuo ha diritto a prendere parte liberamente alla vita culturale della comunità, di godere delle arti e di partecipare al progresso scientifico e ai suoi benefici".
D'altronde, la tecnologia nel Nord del mondo si può sviluppare solo grazie alla protezione della Proprietà Intellettuale e le leggi di ratifica dei Trattati Internet dell'OMPI varate dai Paesi del Nord si inseriscono nella logica del paragrafo due dell'Articolo 27 della Dichiarazione Universale dei Diritti Umani dell'ONU che specifica:

"2. Ogni individuo ha diritto alla protezione degli interessi morali e materiali derivanti da ogni produzione scientifica, letteraria e artistica di cui egli sia autore".
Per uno sviluppo sano e non liberticida di Internet, bisogna dunque cercare di risolvere, almeno in parte, il conflitto tra gli interessi dei creatori e quelli del pubblico introdotta già nel 1948 dalla Dichiarazione Universale dei Diritti Umani dell'ONU, però lasciato ampiamente irrisolto fin da allora.

DELLE LINEE DIRETTRICI DA ESPLORARE

Alcune linee direttrici possono essere studiate in dettaglio. Sono di due categorie: quelle di carattere normativo e quelle di carattere pragmatico.

ASPETTI NORMATIVI

- Appare altamente utile per i Paesi occidentali, Italia inclusa, promuovere una ratifica più generale del WCT e del WPPT, in particolare con i Paesi in sviluppo: tali Trattati offrono una cornice d'inquadramento utile per la Rete in materia di diritto d'autore, e dei margini per lo sviluppo di modelli proprietari ma anche di modelli aperti sicuramente più ampi di quelli scelti ad esempio dai governi occidentali nelle legislazioni esistenti;
- E' altamente auspicabile una modifica delle imperfette legislazioni occidentali (DMCA e soprattutto EUCD) per un migliore equilibrio tra modelli proprietari e modelli aperti, destinato a permettere sia il loro pieno sviluppo reciproco sia una sana concorrenza tra loro, nell'interesse del consumatore come della ricchezza e della diversificazione della Rete

ALTRI ASPETTI

L'attività normativa è spesso in ritardo sui fenomeni economici, culturali e sociali. Questo può essere un freno alla libertà degli individui e al progresso economico, culturale e sociale, ma può anche risultare favorevole alle libertà degli individui e in fin dei conti alla società (la dottrina anglosassone pone spesso l'accento su quest'ultimo aspetto): può dunque anche rivelarsi opportuno non legiferare in eccesso o troppo velocemente su materie nuove come il diritto d'autore su Internet. Rapidissimi cambi tecnologici e anche di business models sulla rete non devono essere frenati da legislazioni eccessive, che definiscono troppo nel dettaglio delle regole che rischiano di diventare rapidamente limitanti e obsolete. Tuttora è necessario per la società avere almeno un inquadramento minimo chiaro del diritto d'autore su Internet, anche tramite misure e soluzioni pragmatiche.

Sarebbe dunque opportuno lavorare in tempi brevi sull'ideazione di meccanismi pragmatici per alleviare la contrapposizione tra creatori e pubblico: potrebbero essere individuate soluzioni e vie pragmatiche a livello mondiale, in parte sviluppate a partire dal modello usato per risolvere le frizioni tra nome di dominio e marchio. Potrebbe essere fatto in materia di Internet e diritto d'autore uno sforzo simile a quello condotto da ICANN e dalla Comunità internazionale alla fine degli anni Novanta del passato secolo per stabilire in materia di cybersquatting e cybergrabbing l'Uniform Dispute Resolution Procedure (UDRP: meccanismo amministrativo uniforme per la risoluzione delle controversie). Lo sforzo consisterebbe nel cercare come estendere l'UDRP oggi relativo ai soli

conflitti tra nome di dominio e marchi (concretamente i conflitti tra il titolare di un indirizzo Internet e il titolare di un marchio simile), dai conflitti sull'indirizzo ai conflitti sul contenuto dell'indirizzo: vale a dire la creazione di un UDRP per risolvere in particolare conflitti tra il titolare di un indirizzo web titolare dei contenuti inseriti sulla sua pagina e l'eventuale titolare di un diritto d'autore violato da questi contenuti. Meccanismi più moderni e automatizzati di quelli dell'UDRP attuale possono essere studiati dagli esperti dei Paesi del Nord del Mondo, laddove la tecnologia esiste, per risolvere tali conflitti in modo lineare e semplice. Qualche investimento tecnico, non ingente, sarebbe sicuramente necessario per sviluppare un metodo e dei supporti informatici. Se dei modelli semplici ma anche tecnicamente sofisticati di gestione del diritto d'autore come "Creative Commons" hanno potuto svilupparsi ad hoc e spontaneamente, ci deve essere però chiaro che dei modelli simili per la gestione dei conflitti in materia di diritto d'autore sono possibili.

Possono essere ideate altre opzioni, come la creazione di meccanismi comportamentali (guidelines, voluntary codes, etc.), realizzate anche dai diversi componenti che assicurano de facto oggi il governo pragmatico della Rete. Esistono nei Paesi del Nord numerosi studiosi che lavorano su questi temi assai importanti da considerare. Inoltre, per quanto riguarda il nostro continente, potrebbe essere promossa la creazione di un progetto specifico di Helpdesk europeo su Internet e diritto d'autore, simile (ed eventualmente collegato) all'utilissimo IPR Helpdesk sviluppato da qualche anno dall'Unione Europea.

IMPLEMENTARE DELLE MISURE PER DIMEZZARE IL GAP NORD-SUD

Il divario Nord-Sud potrebbe essere in parte ridotto dall'ideazione di meccanismi pragmatici per alleviare la contrapposizione tra creatori e pubblico e da UDRP in materia di contenuti e diritti d'autore: infatti, se i governi del Sud del Mondo rammentano la loro difficoltà d'accesso a contenuti in rete protetti dal diritto d'autore e da DRM nei Paesi del Nord, numerosi autori e ricercatori dei Paesi in sviluppo e qualche governo del Sud rammentano le violazioni dei loro diritti d'autore commesse in rete da operatori economici ubicati nei Paesi industrializzati.

Inoltre, l'auspicato sviluppo di guidelines e voluntary codes relativi al diritto d'autore su Internet dovrebbe anche coinvolgere diversi componenti tra i Paesi in sviluppo, con l'obiettivo di rendere più generale e dunque più stabile l'inquadramento informale e autotutelato della relazione di Internet e del diritto d'autore e di contribuire in conseguenza a ridurre il divario Nord-Sud.

Le linee direttrici sopra suggerite sono probabilmente insufficienti per dimezzare il gap Nord-Sud in termini d'accesso ai contenuti. È tramite un impegno più consistente dei Paesi industrializzati a realizzare un vero trasferimento tecnologico e l'assistenza tecnologica ai Paesi in sviluppo, nel senso indicato però finora mai considerato seriamente degli Articoli 7 e 8 dell'Accordo sugli aspetti dei diritti di proprietà intellettuale attinenti al commercio (Accordo TRIPS) nel 1994, che si situa una soluzione che soddisfi le necessità dei Paesi più poveri in una logica di sviluppo sostenibile. Questo non solo per diminuire il divario Nord-Sud ma anche per rendere più fluida al Nord la gestione dei diritti d'autore sul supporto "Internet", nell'interesse dei creatori e di tutta la comunità.

ANTONIO ANSELMO MARTINO

Infoetica

Antonio Anselmo Martino è il curatore del presente Quaderno. Le sue note biografiche sono riportate in PREMESSA.

> *In every system of morality, which I have hitherto met with, I have always remarked, that the author proceeds for some time in the ordinary way of reasoning, and establishes the being of a God, or makes observations concerning human affairs; when of a sudden I am surprised to find, that instead of the usual copulations of propositions, is, and is not, I meet with no proposition that is not connected with an ought, or an ought not. This change is imperceptible; but is, however, of the last consequence. For as this ought, or ought not expresses some new relation or affirmation, 'tis necessary that it should be observed and explained; and at the same time that a reason should be given, for what seems altogether inconceivable, how this new relation can be a deduction from others, which are entirely different from it.* [David Hume, 1739]

I FATTI CHE CAMBIANO CON INTERNET. COME CONVIVERE NELLA RETE

Un modo di concepire lnternet è pensare alla scoperta di una nuova isola [1] bella, grande piena di risorse e alla portata di tutti quelli che vogliono vivere in essa e goderne i beni. La tecnologia informatica è come l'isola. Costituisce un vasto territorio per gli impegni umani. Possiede un enorme potenziale di servizio agli esseri umani, come ambiente del nostro sviluppo. Le regole,

politiche, atteggiamenti e convenzioni che sviluppiamo in relazione con questa tecnologia determineranno completamente se il suo potenziale sarà sfruttato per il bene o per il male. Possiamo sviluppare leggi e politiche per assicurare che questa tecnologia serva all'umanità o possiamo permettere che il suo potenziale sia sprecato. Uno dei problemi più seri che si pongono è come vivere in questa fantastica isola. Ci vogliono delle regole per Internet - e dice bene l'autore citato - come per questa fantastica isola. Chi pone le regole? È il primo problema: quindi il grande problema della rete è il governo di essa.

Ma le regole non vengono a casaccio, si danno per raggiungere uno scopo o più di uno. A questo punto entra l'etica o, se volete, il tema dei valori. Quali valori difendere per ottenere cosa? con quali mezzi? da chi? per quanto tempo?

LE REGOLE CERCANO SCOPI, GLI SCOPI PRIVILEGIANO VALORI

Una cosa è certa: la massimizzazione di qualsiasi valore va a detrimento degli altri. Anche i fantastici valori della rivoluzione francese, se uno di loro fosse massimizzato, sarebbe a detrimento degli altri due. A questo punto sappiamo che ragione vuole sapere quanta fratellanza, con quanta libertà e in quale uguaglianza. Sostenere un valore è funzione delle ideologie ma con le ideologie non si riesce a convivere, se non con prezzi sociali molto alti.

Premetto che per me il valore massimo è la libertà. Ma curiosamente per difenderla devo accettare posizioni che libertarie non sono. Il problema si pone quando la non libertà degli altri viola la mia libertà. O, detto in altri termini, quando e come porre dei limiti a coloro che non sono non libertari.
Sgombero subito il campo dicendo di essere un non cognitivista etico, vale a dire uno che non ammette che un valore qualsiasi o un insieme di valori possano essere provati come "naturali", "derivati della parola di Dio", "cogenti perché razionali", ecc.. Ammettere che non si possa provare la verità o vigenza di un sistema di valori qualsiasi, non significa essere indifferenti nella lotta politica o civile. Si può essere non cognitivista etico e allo stesso tempo uno sfegatato difensore di un valore o un insieme di valori tale da giustificare di mettere a repentaglio la propria vita. È una posizione scientifica con riferimento alla possibilità di fondare valori ultimi: alcuni pensano che sia possibile, quindi sono cognitivisti etici, altri pensiamo che non sia possibile, quindi siamo non cognitivisti etici [2].

L' INFOETICA

L'infoetica è stata la vaga idea di alcune persone e alcuni pochi convegni organizzati dalle Nazioni Unite con questo nome. Una delle prime, nel 1999 a Parigi, buttò sul tappeto i temi più urticanti dell'etica in Internet. Se si guardano i temi posti allora, essi non sono molto diversi da quelli che ci poniamo ora: il multilinguismo, il divario digitale, la governabilità della rete o, detto in modo positivo, favorire il multilinguismo, l'accesso a Internet, la collaborazione tra le nazioni, tra i governi e le imprese e la società civile. Si chiese di fare delle consultazioni al fine di preparare un progetto di raccomandazioni alla successiva Conferenza Generale.

Anche l'Unione Europea si è posta il problema di un'etica per l'Internet e, a tali fini, ha organizzato convegni, sviluppato ricerche e ha avviato qualche progetto di direttiva. In tema di diritti d'autore e protezione della proprietà intellettuale si è pronunciata l'Unione Europea [3]. Anche si sono tenute importanti riunioni a livello accademico, come quella organizzata dalla Università Luiss di Roma, che ha svolto nel '99 la quarta edizione di "Ethicomp", Conferenza internazionale sull'impatto sociale ed etico delle tecnologie per l'informazione e la comunicazione.

Ethicomp99 si è articolata in una giornata introduttiva (che ha spaziato dalla storia del computer ethics, a computer ethics e imprese, dal problema della gestione dei dati personali in Usa, all'impatto di Internet dal punto di vista etico sul lavoro, a casa, nell'educazione) seguita da una novantina di interventi su ricerche specifiche, e si è conclusa con un paio di tavole rotonde e due relazioni a invito del presidente dell'Autorità per la protezione dei dati personali Stefano Rodotà [4] e di Deborah Johnson [5] del Georgia Institute of Technology. Quest'ultima ha tracciato il "Futuro del computer ethics nel XXI secolo", mettendo in risalto come saranno cruciali nei prossimi anni da un lato la definizione di regole giuridiche e la loro armonizzazione a livello internazionale, dall'altro la creazione di un sistema di "fiducia" che favorisca gli scambi via Internet tra i vari soggetti (individui, società, istituzioni...) con adeguate garanzie di sicurezza. La computer ethics come disciplina a sè stante sarebbe invece destinata presumibilmente a scomparire, giacché quel che conta non è la tecnologia in sé, bensì ciò che con la tecnologia gli individui e le istituzioni fanno, così come è sempre stato con gli strumenti di cui l'uomo via via si è dotato.

L' ETICA NELLA RETE

Che la computer ethics sopravviva o no in futuro è tutto sommato domanda oziosa, stante il fatto che l'introduzione della tecnologia solleva oggi problemi dei quali è essenziale prendere coscienza, anche perché le regole giuridiche non sono sufficienti. Le tecnologie non sono affatto neutre. Lo ha sottolineato Stefano Rodotà, che autorevolmente ha svolto un ruolo di garante in un Paese dove le

questioni etiche paiono non godere generalmente dell'attenzione dovuta, quasi si trattasse di una disciplina "astratta", buona solo a usi di facciata, mentre è vero il contrario. Tensioni tradizionali oggi si acuiscono e ad esse se ne aggiungono di nuove: particolarmente stringente per quanto riguarda Internet è la necessità di tutelare i diritti fondamentali a fronte delle logiche del controllo e del mercato. Il che non può avvenire attraverso una disciplina solo nazionale; i confini dello Stato svaniscono nella rete, materializzazione visibile della cosiddetta globalizzazione. Ci vogliono invece principi comuni e possibilmente una sorta di Carta dei diritti internazionalmente riconosciuta.

Prioritario rimane il principio della dignità umana da cui discendono innanzitutto il problema dell'uguaglianza (chi sono/saranno gli esclusi?) e la necessità di ridefinire i criteri che qualificano una società democratica. Tale è per Rodotà la società che promuove l'inclusione, non solo attraverso un'opera di alfabetizzazione, bensì permettendo ai cittadini di sviluppare una capacità critica nei confronti delle nuove tecnologie. Questo, per una società che voglia definirsi democratica, deve dunque diventare un cardine delle politiche pubbliche, accanto a quello della trasparenza della società (e non dell'individuo che deve invece aver tutelate sia la sfera privata sia la libertà di esprimersi attraverso la rete), ovvero possibilità di controllo e di partecipazione da parte dei cittadini.

La funzione dell'etica nella rete si impone perché questa è pervasiva e perché presenta situazioni fino ad oggi sconosciute. Chi gestisce le reti telematiche ne controllerà anche i contenuti? Quali sono i diritti fondamentali nell'Information Society? Come garantire l'accessibilità e superare il digital-divide? Come selezionare i contenuti in una rete dominata da servizi commerciali o di entertainment? Come affrontare il dilemma tra beni comuni e copyright? Come garantire la sicurezza delle informazioni e la privacy? E poi ancora il dilemma tra innovazione tecnologica e affidabilità dei computer, tra etica hacker e reati informatici, tra ricerca di base e intelligenza artificiale [6]. E nelle aziende i manager si trovano a dover decidere i "codici etici per il personale interno" e si trovano a dover integrare questi strumenti con rigorose policies aziendali per trattare i dilemmi etici con i quali i computer professionals impattano quotidianamente: dall'Internet governance all'accessibility, dalla privacy al copyright, dall'uso appropriato dell'informatica in azienda alla gestione della conoscenza, dai reati informatici alla security ed agli hacker, dall'affidabilità dei computer al loro impatto sugli ecosistemi, dall'intelligenza artificiale alle applicazioni militari [7].

L'associazione Politeia, attraverso una sezione che dirigono D'Orazio e Patrignani, si sta occupando in Italia del tema della Computer Etichs e in questo momento sono impegnati in lavori per definire 13 punti che devono caratterizzare questa disciplina [8].

LA FUNZIONE DEI VALORI NELLE REGOLE. OCCIDENTE E ORIENTE

Torniamo al tema dei valori e delle regole. Valori e regole in un mondo globalizzato. Valori che stanno dietro alle regole e giustificano gli obiettivi.

Credo che dal punto di vista sintattico vi sia una logica valida per Oriente e Occidente. La logica occidentale ha ormai raggiunto un grado straordinario di sviluppo, ma sostanzialmente è sostenuta nella vecchia definizione aristotelica: Il passaggio da un insieme di enunciati ad un enunciato, necessariamente [9].

In logica occidentale è praticabile la formula 2n quando i termini che si mettono in gioco sono due e "n" è il numero variabile di casi nei quali occorrono tali termini. Questo è facilmente comprensibile in qualsiasi sistema binario [10]. Nella logica orientale è molto difficile prescindere dalla consultazione del libro del Yi King (o I Ching); questo libro contiene degli esagrammi. Un esagramma è un insieme di linee complete o divise in sei righe. Dato che continuo o diviso sono due termini e 6 le linee od occorrenze, vale anche la formula 2n dove n=6, vale a dire 64. E sessantaquattro sono gli esagrammi dell' Yi King o libro delle mutazioni.

La similitudine di queste sintassi consente di dire che tanto in oriente quanto in occidente, dal punto di vista logico, si ragiona in modo analogo e una spiegazione possibile è il modo di essere conformato il cervello umano. Questo ha consentito la rapida diffusione delle nuove tecnologie che sono sostanzialmente sintattiche in occidente ed oriente. Per essere tosto va detto che la logica è anteriore alla matematica o alla geometria che sono interpretazioni di un tipo di logica.

Più complicate sono le cose dal punto di vista semantico: un termine sempre trova senso dentro un contesto e i contesti sono culturali e storici. Vi sono più di seimila lingue nel mondo quindi è molto difficile pensare ad una semantica unica. Comunque i lavori più moderni in questo campo cercano di trovare questa semantica primigenia.

Il tema diventa ancor più complicato dal punto di vista pragmatico e quindi è comprensibile che vi siano diversi sistemi di valori. Ciononostante, se si va a cercare nelle diverse culture un insieme di

valori primari rilevanti, è possibile trovare delle compatibilità. Tra i precetti ebraici, cristiani, musulmani e le paramite [11] buddiste è possibile trovare elementi comuni da poter enunciare in modo generale [12].

NECESSITÀ DI UN'ETICA MINIMA GENERALMENTE CONDIVISA

La cosa più difficile è quella di tentare un'etica minima comune in un mondo globalizzato dove le differenze non sono abissali, ma sono fortemente caratterizzate da una cultura e una soluzione. Eppure non vi sono alternative. Bisogna trovare un numero minimo di regole etiche di convivenza applicabile in oriente come in occidente nonostante le diversità di lingue, tradizioni e culture.

Non si tratta di un'operazione sintattica, ma pragmatica, quindi piena di difficoltà, ma non impossibile. La prima cosa che ci vuole è accettare gli altri, vale a dire accettare che vi siano persone, comunità, culture che non la pensano come noi riguardo a molti temi importanti. Questo apre uno spiraglio importante verso il dialogo e il dialogo è l'unica via possibile per arrivare ad accettare un'etica minima anche nella Rete. Capisco bene che non si tratti di una area facile, ma escludo che sia impossibile.

Attualmente, di fronte al crollo di alcune ideologie politiche, risorgono altre con forte accento religioso. Le religioni sono temi molto importanti per essere trattate superficialmente, ma in questo caso mi occupo solo della possibilità di dialogo interreligioso, dialogo possibile - come dicevamo prima - solo a condizione di accettare l'altro in quanto tale. Questo dal punto di vista teorico è sostenuto in modo impeccabile da Adriano Fabris: "Emergono dunque qui delle alternative ben precise: l'alternativa fra una concezione nella quale il particolare è già da sempre universale e quella secondo la quale esso può diventarlo, attraverso l'esperienza di vita e l'impegno dell'uomo religioso; l'alternativa fra una concezione estensiva e una intensiva del rapporto tra particolare e universale. Rispetto a loro bisogna fare chiarezza, per mostrare che non c'è un unico senso di "universale", che non c'è un unico modo per pensare il rapporto tra la propria visione particolare, comunque ritenuta vera, e quella degli altri. A partire da qui bisogna far nascere e sostenere, all'interno di ciascuna religione, quelle concezioni che scelgono una versione non esclusiva dell'universale, e che perciò possono promuovere il dialogo invece dei conflitti. E soprattutto, assumendo questa prospettiva, possiamo dunque, sia che crediamo oppure no, pensare la possibilità di un Dio condiviso e operare per la pace. Ciascuno partendo dalle sue scelte; ciascuno in base alle sue idee" [13].

Dal punto di vista pratico si tratta di riflettere sulle regole principali delle tre religioni monoteiste e il buddismo. Me ne rendo conto che è un atto di semplificazione barbaro, ma d'altro canto i tempi stringono e le persone di questo pianeta hanno sempre più bisogno di soluzioni semplici che si possano raggiungere senza troppi intoppi. L'idea di paragonare le regole di convivenza etica di queste quattro religioni è perchè con loro si copre la maggior parte del pianeta. È vero che rimangono fuori molte religioni che non sarebbe né giusto né ragionevole ignorare, ma è anche vero che, una volta stabilita una quantità minima di regole etiche compatibili tra queste quattro religioni [14], le altre possono proporre le loro differenze e/o similitudini e far anche parte di questo dialogo multiplo al quale si vuole arrivare.

Le regole di convivenza etica delle tre religioni monoteiste sono facilmente riconducibili ad una quantità di regole comuni che ne derivano anche dalla comune origine. I paramiti del buddismo ovviamente sono espresse in modo diverso, ma si possono trovare le concordanze a livello di regole. Colpisce il fatto che le regole delle religioni monoteiste siano delle proibizioni, mentre i paramiti sono permessi, obblighi o facoltà. Dal punto di vista della logica etica si equivalgono non così dal punto di vista pragmatico. Ma anche qui le coincidenze si trovano facilmente e tutto al più si trova come differenza la vocazione buddista di occuparsi del benessere non solo degli uomini "ma di tutti gli esseri viventi" [15].

CERCARE I VALORI E ADATTARE LE REGOLE, SEGUIRE DELLE BUONE PRACTICIES E ARRIVARE AI VALORI.

Questa è una via possibile complessa che i più stanno percorrendo per il mondo, se accettiamo una via kantiana di imperativi assoluti, complessa soprattutto da applicare poi nei casi concreti, ma efficace per far vedere la fondazione teorica di quanto si sostiene.

Una via contraria, vale a dire non kantiana, è quella indicata da David Ross [16] il quale sostiene che noi abbiamo solo obblighi morali "prima facie", vale a dire essendo la nostra conoscenza limitata, noi abbiamo obblighi morali conformi ai dati che ci sono stati forniti, quindi "prima facie"; se poi altri dati vengono ad alterare il contesto informativo, è possibile che vi sia un mutamento nel nostro obbligo morale. Questa è la ricerca delle best practicies in ogni contesto, vale a dire un modo quasi induttivo di valutare una condotta morale. Le due metodologie sono valide e si integrano tra di loro. La deduttiva consente di paragonare più condotte, l'induttiva permette di incorporare le pratiche che ci sono già e insieme fanno ben funzionare una società civile come quelle relative alla responsabilità sociale delle imprese.

Se questo è possibile, se è possibile cercare regole minime di convivenza che possano essere accettate tanto in oriente quanto in occidente per mezzo delle due metodologie indicate, possiamo passare il tutto alla infoetica e dire che la concentrazione maggiore nei prossimi anni sarà quella di costruire un sistema di regole minime di convivenza in Internet che possa essere accettata da tutti gli utenti, incominciando dalla comunità di vedute delle tre religioni monoteiste ed il buddismo estendendola poi ad ogni forma di regola morale che sia in vigore in qualsiasi parte del pianeta purché riconducibile ad alcuna delle regole già indicate o essere aggiunta ad esse con gli stessi criteri con i quali sono nate le prime.

Contemporaneamente possiamo accettare quelle "buone consuetudini" che hanno permesso la pacifica convivenza e hanno risolto i conflitti nati all'interno della Rete.

L' INFOETICA IN UNO STATO DI DIRITTO

L'importanza della infoetica è evidente. Le norme giuridiche cercano di trovare il modo di risolvere i conflitti pacificamente indicando obiettivi e il modo di ottenerli. Sulla ricerca degli obiettivi ed il modo di raggiungerli l'infoetica deve essere il metodo privilegiato di arrivarci. La citazione di Hume dell'inizio sta giustamente ad indicare che non basta avere un'enorme quantità di dati sul mondo, sull'essere, ci vuole qualcuno, almeno uno, su come vogliamo che sia il mondo sul dover essere. È questo proprio lo spartiacque.

Tocca all'infoetica trattare gli argomenti normativi del dover essere della Società dell'informazione facendosene carico nel maggior numero di paesi possibili, nella varietà dei contesti sociali, politici e culturali dove essi si sono sviluppati e nel modo necessario per stabilire un dialogo sulla validità di tali obiettivi etici e delle norme giuridiche per raggiungerli.

Il primo problema che si pone è quello della governance della rete e della governance nella rete, poiché si devono trovare i modi perché i poteri pubblici sentano l'obbligo di consentire la maggiore circolazione della informazione, anche propria, tentare di eliminare le ragioni economiche che impediscono ad una parte importante della popolazione di avere accesso a questa informazione e togliere tutte le barriere in modo tale di rendere effettivo il "diritto a comunicare" e l'uso della rete per far circolare la cultura, la scienza e la formazione.

Il secondo è relativo ad un concetto tipicamente giuridico, ma che piano piano può costituire la meta dell'infoetica se pensata per una società democratica: il rispetto dello stato di diritto.

Può sembrare un obbiettivo minore e legato al formalismo dei giuristi, invece guardando lo stato attuale del pianeta è sempre di più una conditio sine qua non per la democrazia.

Il terzo è relativo alla protezione della dignità umana nell'era digitale. Un insieme di regole e best practicies adottate dai poteri pubblici, le imprese e la società civile tendenti a preservare la dignità umana dalla prepotenza del potere, delle grandi risorse e della forza organizzata. Regole di sicurezza per l'individuo, la sua vita privata e la libertà di espressione.

NOTE

[1] Johnson, Debora G.: Computer ethics. Englewood Cliffs, N.J. : Prentice-Hall, c1985, p. 13. "Un'analogia che può derivare da utilità... consiste nel pensare ai computer, ai sistemi informatici, e alla tecnologia informatica come un'isola appena scoperta. Supponiamo, nel caso dell'isola, che nessuno sapesse che esisteva, quando fu scoperta da una squadra internazionale di esploratori. È disabitata, ma è molto abitabile. È ricca in risorse naturali, ha un clima temperato durante l'anno, etc. La notizia della scoperta ha generato un gran interesse in tutto il mondo e molti individui ed imprese vogliono stabilirsi lì. Chi vuole trasferirsi vede il suo enorme potenziale. Alcuni vedono l'isola come un'opportunità per costruire una nuova società, un modello di democrazia mondiale, non nazionalista. Altri vedono il potenziale di sfruttamento delle risorse naturali dell'isola; altri poi contemplano il potenziale di sviluppo dell'isola come centro internazionale di turismo. La lista di usi potenziali dell'isola può aumentare…"

[2] A. A. Martino, Valores: ética y metaética, in A. Martino, E. Russo, L. Warat, Temas para una filosofía Jurídica, Cooperadora de Derecho y Ciencias Sociales, Buenos Aires, 1974, pp. 109 /176.

[3] Libro Verde – I diritti di autore e i diritti connessi nella Società dell'Informazione COM(95) 382, Luglio 1995. 1#obiettivo Inquadrare vari problemi in materia di diritti d'autore e diritti perfezioni nel contesto dello sviluppo della Società dell'Informazione, con oggetto in questione di determinare le misure legislative necessarie. 2#misura COMUNITARIA Libro Verde della Commissione Europea, di 27 di Luglio di 1995, sui diritti d'autore ed i diritti perfezioni nella Società dell'Informazione. 3#contenuto Detto Libro si compone di due capitoli. Nel primo si descrive il funzionamento teorico della Società dell'Informazione. Sottolinea l'importanza dello

sviluppo della Società dell'Informazione per la Comunità Europea e, in questione, si mostra come si iscrive il suo sviluppo nella cornice giuridica del Mercato Interno. In detta parte si tenta di determinare le sfide che la realizzazione della Società dell'Informazione comporta. Nel secondo capitolo, la Commissione, basandosi sulle contribuzioni dei settori interessati, ha determinato nove temi nella sua opinione prioritari per i regimi di protezione dei diritti d'autore e diritti perfezioni di fronte al funzionamento della Società dell'Informazione. La Commissione desidera richiamare l'opinione dei settori interessati sugli aspetti tanto tecnici come normativi delle questioni per determinare le misure legislative necessarie.

[4] http://www.swif.uniba.it/lei/rassegna/rodot%C3% A0.htm

[5] http://www.swif.uniba.it/lei/rassegna/johnson.htm

[6] Roberto Patrignani in una conferenza alla Scuola Normale Sant'Anna di Pisa "Introduzione alla Computer Etichs" Vedi http://www.politeia-centrostudi.org/eticaIT.html

[7] http://www.politeia-centrostudi.org/eticaIT.html

[8]

Opportunità e processi democratici nel cyberspazio
Cittadinanza digitale o e-democracy
e-government
Accesso universale e Divario Digitale
Tecnologia dell'informazione e della comunicazione e posti di lavoro
Contenuti della Rete e processi educativi
Diritto d'autore sui contenuti digitali
Difesa dai rischi di intrusione nei sistemi informatici
Diritto alla protezione dei dati personali o Affidabilità dei computer
Crimini informatici e virus o Intelligenze artificiali, robotica e nanotecnologie
Conflitti e guerre
Salvaguardia dell'ambiente e riciclaggio tecnologie
Internet Governance
Realtà virtuale e giochi online http://www.politeiacentrostudi. org/ricercheincorso.html

[9] Aristotele aggiungeva “enunciati veri” ed “enunciato vero”. Credo che la definizione proposta togliendo i termini di “verita” siano più adeguati agli studi attuali. Vedi . MARTINO, Antonio Anselmo; ALCHOURRON, Carlos E. Logica senza verità sta in: AA.VV Sistemi Esperti Giuridici l'Intelligenza Artificiale applicata al Diritto. A cura di Paola Mariani e Daniela Tiscornia Milano, Franco Angeli, 1989, p. 277 – 303 "Analisi automatica del linguaggio. 55.2" MARTINO, Antonio Anselmo; ALCHOURRON, Carlos E. Logique sans verité sta in: Revue Internationale de Semantique Juridique. Vol. III. F. 7 - 1989, p. 33. MARTINO, Antonio Anselmo; ALCHOURRON, Carlos E. Logic Without Truth sta in: PATTARO, Enrico (a cura di), Ratio Juris, An International Journal of Jurisprudence and Philosophy of Law, vol. 3, n. 1, marzo 1990, Basil Blackwell Oxford and New York. MARTINO, Antonio Anselmo LEGAL EXPERT SYSTEMS sta in: T.D. Campbell, R.C.L. Moffat, S. Sato, C. Varga (a cura di) Archiv für Rechts- und Sozialphilosophie, Beiheft 39, 1991,Franz Steiner Verlag, Stuttgart.

[10] La prima versione di un sistema binario compare in Liebniz, sulla presenza di Dio nel mondo. Infatti, Leibniz non credeva nel diavolo e diceva che il bene era la presenza di Dio nel mondo, il male la sua assenza. E che questo poteva essere simboleggiato con due numeri 1 e 0 e che con questi due numeri si poteva rappresentare tutta la conoscenza umana. Per dare un esempio rappresenta i primi 8 numeri della successione fondamentale con O e 1, creando un sistema binario.

[11] E' il termine adoperato dai buddisti per riferirsi agli insegnamenti sul modo di comportarsi. Si tratta di un termine sanscrito adoperato da Nagarjuna per spiegare gli insegnamenti di Budda.

[12] Questo è un tema molto complesso e sul quale esiste già una bibliografia estesa. Non è il caso di trattarli qui.

[13] Adriano Fabris, Perspectivas del diálogo interreligioso (o sea: El dios compartido) in www.iiefgs.org Seminarios de la Universidad de Pisa. La traduzione appartiene all’autore.

[14] So benissimo che i buddisti negano che la loro sia una religione ma non è questo il punto per discuterlo.

[15] Chogye Trichen Rinpoché, Separarsi dalle quattro affezioni, Edizioni Dharma, Buenos Aires, Gli insegnamenti sono basilari e un po’ criptici e indicati in termini negativi perché le quattro affezioni sono considerate cattive per l’uomo praticante: 1. Se ti affezioni a questa vita non sei un

praticante; 2. Se ti affezioni a samsara non hai rinuncia. 3 Se ti affezioni ai propri interessi non hai la mente dell'illuminazione, 4. Se c'è fissazione non hai la visione. Una volta espressi possono essere poi trascritti nella parte positiva dei paramiti.

[16] 16 D. Ross, Etics, London, 1930

AGENDA DI TUNISI ART.72 THE MANDATE OF THE IGF

a. Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.

b. Facilitate discourse between bodies dealing with different cross-cutting international public policies regarding the Internet and discuss issues that do not fall within the scope of any existing body.

c. Interface with appropriate intergovernmental organizations and other institutions on matters under their purview.

d. Facilitate the exchange of information and best practices, and in this regard make full use of the expertise of the academic, scientific and technical communities.

e. Advise all stakeholders in proposing ways and means to accelerate the availability and affordability of the Internet in the developing world.

f. Strengthen and enhance the engagement of stakeholders in existing and/or future Internet governance mechanisms, particularly those from developing countries.

g. Identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations.

h. Contribute to capacity building for Internet governance in developing countries, drawing fully on local sources of knowledge and expertise.

i. Promote and assess, on an ongoing basis, the embodiment of WSIS principles in Internet governance processes.

j. Discuss, inter alia, issues relating to critical Internet resources.

k. Help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users.

l. Publish its proceedings.

ANDREA MONTI

Internet: quando le regole “dal basso” piovono “dall’alto”

Andrea Monti, - a.monti@amonti.eu Avvocato, si occupa di bioinformatica, diritto delle telecomunicazioni e delle tecnologie dell'informazione. Già componente del gruppo ITA-PE e poi del Comitato esecutivo della Naming Authority italiana, è past-president di ALCEI (Associazione per la Libertà nella Comunicazione Elettronica Interattiva). Svolge regolarmente attività accademica. È l'ideatore della Italian Biotech Law Conference, giunta - nel 2007 - alla terza edizione. Ha collaborato e collabora con diverse università (in particolare, con quelle di Chieti e di Milano) e ha pubblicato i suoi articoli su riviste scientifiche internazionali e italiane. Ha presentato relazioni in convegni organizzati in USA, Inghilterra, Francia, Belgio, Repubblica Ceca, Svizzera, Bulgaria. Ha effettuato docenze su computer crime e diritto d'autore per le scuole delle Camere penali, e per le strutture di formazione delle forze di polizia come l'Istituto superiore della Polizia di Stato, il Centro addestramento Polizia postale, il Centro nazionale amministrativo dell'Arma dei Carabinieri. Giornalista-pubblicista, cura sulla testata PC Professionale una delle più longeve rubriche italiane che si occupano di rete e di legge. Articoli e interviste su questi temi sono stati pubblicati dai maggiori quotidiani e periodici italiani, come La Repubblica e IlSole24Ore. Ha scritto per l'editore Apogeo insieme a Stefano Chiccarelli il libro "Spaghetti Hacker" e "Segreti, spie, codici cifrati" con Enrico Zimuel e Corrado Giustozzi. Sempre per Apogeo ha curato la traduzione italiana del libro di Alan Cooper "The inmates are running the asylum" edito con il titolo "Il disagio tecnologico". Per Hops editore, insieme a Alessia Ambrosini, ha scritto "Trademark online". Il suo blog www.ictlex.net - dove raccoglie riflessioni e materiali sul diritto, sulla politica e sulla cultura della rete fin dal 2000 - è stato premiato da Reporter sans frontiéres con il Freedom Blog Award 2005.

INTRODUZIONE

Con una frequenza oramai allarmante la "ontologizzazione" della tecnologia - e dell'internet, per quanto ci interessa in questa sede - condizionano le strategie economiche, le analisi (non solo) politiche e le scelte normative. Sembra proprio, in altri termini, che sia diffusa la convinzione che da qualche parte esista un "Mr. Internet" dotato di autonoma esistenza e individualità, in grado di sovvertire le regole del mercato e di rendersi responsabile dei crimini più efferati - dall'eversione alla perversione. Analogamente, dunque, "Mr. Internet" può ben essere il destinatario di anatemi, crociate e leggi ad personam. La "personificazione" dell'internet rende la vita del repressore molto più semplice. Nessuno prenderebbe sul serio chi proponesse - o invocasse - una legge per vietare la pubblicazione di manuali universitari di chirurgia o anatomia. Ben altro accadrebbe se le stesse identiche informazioni fossero rese disponibili tramite qualche newsgroup o qualche sito web non

accademico e qualche "associazione di consumatori" scandalizzata dal disgusto provocato dalle immagini in questione ne chiedesse la distruzione. In questo caso, infatti, chi chiedesse di rimuovere per legge quelle informazioni "pericolose" troverebbe sicuramente moltissime persone disposte ad ascoltarlo. "Dare la colpa all'internet" per legittimare censura e repressione - o per giustificare la necessità di nuove leggi - è un vero e proprio atto di disonestà intellettuale e di pavidità politica.

Conseguenza inevitabile di questo presupposto culturale è stata la proliferazione di quella che Isaac Asimov chiamò la "Sindrome di Frankestein " [1]. Nel corso degli anni questa "patologia" si è manifestata nelle forme più svariate, dai tracolli economici (peraltro ampiamente prevedibili) [2], a una repressione bieca e ignorante [3]. Non che questo sia accaduto out of the blue: le avvisaglie del futuro prossimo venturo furono denunciate fin dagli anni '90 [4], ma senza suscitare alcuna apprezzabile reazione persino in quella sottile "fetta" di intellettuali e politici che sembravano meno disattenti alla realtà circostante.

MR. INTERNET... CHI È COSTUI?

Ovviamente, non esiste un "Mr. Internet" e non c'è alcuno "spettro nel computer" che minaccia la nostra esistenza. Esistono soltanto - ma è già abbastanza - emuli di Torquemada, di Pinochet e dei Robber Baron che usano gli strumenti a loro disposizione [5] per proteggere la propria esistenza e perseguire i loro loschi fini. Ci sono masse di delinquenti che hanno semplicemente adattato il loro modus operandi alle opportunità rese possibili da nuovi strumenti [6]. E ci sono politici che hanno mostrato tutta la loro insufficienza culturale nel confrontarsi con un potentissimo strumento, cercando di bloccare a ogni costo le nefaste - per loro - conseguenze della circolazione libera di informazioni (vale a dire la possibilità del controllo democratico diretto).

Come scriveva nel 1996 Giancarlo Livraghi, "parte spesso da costoro il concetto di una società in pericolo, di una rete affollata di hacker e pirati, o peggio ancora (che cosa terribile!) di opinioni liberamente diffuse che danno voce anche alle minoranze, al dissenso, o comunque a quel "profano volgo" cui finora era solo consentito di inchinarsi tremante davanti al potere di chi tiene le chiavi della Legge (e dell'informazione) ." [7] Queste considerazioni non devono, in realtà, stupire più di tanto se ancora nel 2002 era possibile rilevare che: "Italy's legal and political system doesn't have a sound tradition of understanding technology, science and innovation. This is a country that started recovery from "practically zero" at the end of World War Two. It was still basically an agricultural

economy, its (limited) industrial resources were destroyed. As late as 1960 there was still a high rate of illiteracy. Technological development was far behind most of Western Europe.

"Of course there were, and there are, leading personalities in the world of science and technology. And there are Italian companies, large and small, with strong technological advancement in their specific fields. But in the world of politics and law, and in a large part of the academic establishment, there never was an osmosis between the development of science and technology and the perception of government, legislation and society. Old-fashioned ideas, dating back to Italy's pre-industrial culture, still influence the thinking of people in government and parliament - as well as schools, the intellectual élite and a large part of the citizenship. This environment has favored the lobbying pressures by major economic forces that have been able to influence legislation (and, to some extent, public opinion) in favor of their private interests, at the expense of civil rights and freedom of expression." [8]

Benché siano trascorsi quasi dieci anni, le considerazioni appena riportate conservano appieno la loro attualità (come dimostrano i recenti dati pubblicati nel Sesto Rapporto CENSIS del dicembre 2006) e forniscono una chiave di lettura per spiegare gli sviluppi recenti - a livello globale - delle strategie repressive dei poteri pubblici.

Horror vacui

Dal punto di vista del "potere" in senso lato, gli elementi più destabilizzanti introdotti dalla diffusione delle tecnologie della comunicazione sono, innanzi tutto, l'impossibilità di prevedere da dove arriverà il prossimo "oggetto volante" e l'estrema difficoltà di capire se sia una minaccia, un'opportunità [9] o una bufala. Altro fattore "eversivo" è la possibilità di creare network di persone che possono far circolare informazioni e contenuti [10] in gran quantità - a volte illegali, molto più spesso semplicemente "sgradite" - oltre che creare servizi che si "appoggiano" a quelli offerti dalle grandi imprese e che sfuggono alla regolamentazione vigente [11].

A CHE SERVE LA LEGGE?

Dunque, lo scenario che si presenta può essere descritto in questo modo: da un lato c'è un oceano di informazione che fluisce liberamente e senza una reale possibilità di incanalamento. Dall'altro ci sono pubblici poteri che percepiscono la pericolosità dell'essere - forse per la prima volta nella storia - direttamente controllabili da parte dei cittadini. Non stupisce che trovandosi in una posizione scomoda, potenzialmente in grado di realizzare la favola del "Re nudo" i "grandi poteri" -

ma anche i burocrati locali - cerchino di fare di tutto per ritornare nell'ombra e continuare i loro maneggi, lontani dal fastidio di dover rendere immediatamente conto del loro operato.

È evidente che la soluzione finale a un problema del genere passa per l'eliminazione culturale e giuridica della possibilità per le persone di aggregarsi in gruppi di pressione.

Il primo obiettivo è perseguito con la "televisionizzazione" dell'internet. Cioè con l'appoggio alla realizzazione di piattaforme di distribuzione di contenuti passivi (dal web, al video on demand, alla internet TV) e dunque con l'eliminazione sistematica delle componenti interattive della rete che consentono, appunto, forme di aggregazione politica e civile.

Il secondo obiettivo è perseguito con la asserita necessità di prevenire minacce - presunte o costruite a tavolino - che si traduce nel tentativo di regolamentare, imbavagliare e imbrigliare quello che sfugge al controllo. E qui casca l'asino: i tempi normalmente richiesti per l'emanazione di nuove leggi sono troppo lunghi rispetto alle necessità immediate - dal tacitare la "piazza" al "dire qualcosa" - del politico di turno o del componente dell'Esecutivo. Bisognava dunque trovare un sistema rapido ed efficiente.

LE REGOLE DAL BASSO CHE ARRIVANO DALL'ALTO

La soluzione giuridica al problema è rappresentata dal diffuso ricorso ai "codici deontologici" e alla "autoregolamentazione" fortemente auspicato anche dall'Unione Europea. E dunque il potere politico prende la palla al balzo e sfrutta questo Cavallo di Troia per interagire direttamente con il mondo delle imprese imponendo - al di là di leggi e competenze - ciò che vuole [12]. Il prototipo di questa strategia manipolativa arriva dagli Stati Uniti [13], ed è stata poi applicata - peggiorandola - anche in Italia. Fin dal 2005, grazie al discutibile credito attribuito a "statistiche" [14] sui fenomeni illeciti commessi tramite l'internet a una malintesa interpretazione del concetto di "autoregolamentazione", i ministeri dei beni culturali e delle comunicazioni stanno di fatto condizionando le imprese e i diritti degli utenti senza che il Parlamento possa - o voglia - minimamente intervenire.

Come è noto l'autoregolamentazione - nota anche come "autodisciplina" - è una sorta di "trattato privato" che le aziende di un determinato settore decidono spontaneamente di predisporre e firmare. Lo scopo dell'autodisciplina è quello di dare alle imprese delle regole comuni di comportamento, andando a colmare dei vuoti normativi o estendendo leggi più favorevoli anche a situazioni in cui

questo si potrebbe evitare. L'autodisciplina, inoltre, serve a mettere a disposizione dei soggetti interessati (consumatori compresi, dunque) uno strumento agile, imparziale e competente per decidere su controversie che se fossero trattate in un contenzioso ordinario sarebbero risolte in tempi molto più lunghi e senza la ragionevole certezza che il magistrato incaricato possieda le effettive cognizioni per decidere su materie molto particolari.

Se escludiamo le "procedure di riassegnazione" per i nomi a dominio .it che non possono essere considerate frutto di autoregolamentazione per via dell'incerto statuto giuridico dell'intero sistema di gestione del Registro italiano [15], il caso più antico e importante di autoregolamentazione è il Giurì dell'autodisciplina pubblicitaria. Questo organo, creato per volontà delle stesse imprese che operano nel settore della comunicazione, ha acquisito da subito estrema autorevolezza perchè le imprese ne avevano capito l'utilità - specie per quanto riguarda il delicato problema della "certificazione" della competenza tecnica del soggetto chiamato a decidere.

Fin qui nulla di strano dunque, anzi il modello appena descritto sembrerebbe il vero e proprio "uovo di Colombo" per risolvere molti problemi del settore internet e TLC. E invece, la versione moderna della "autoregolamentazione" diventa "co-regolamentazione", un eufemismo del politichese che - in pratica - significa ingerenza dell'esecutivo nella gestione di un comparto industriale e - indirettamente - emanazione di regole per i cittadini vincolanti al pari di una legge.

"auto" E "co": PREFISSI DIVERSI, STESSO SIGNIFICATO?

Il "padre ignobile" delle "auto-co-regolamentazioni" è sicuramente il famigerato "Patto di Sanremo" [16] risalente al 2005 ufficializzato dai ministeri dei beni culturali, dell'innovazione e delle comunicazioni e che chiedeva a internet provider, titolari dei diritti d'autore e piattaforme di distribuzione, la predisposizione di "codici deontologici" per la "lotta alla pirateria". In realtà l'obiettivo di quel codice era imporre - o meglio, far si che i fornitori di servizi internet "spontaneamente" decidessero - di favorire le azioni giudiziarie promosse dai titolari dei diritti d'autore contro i propri clienti. Il "Patto di Sanremo" fu oggetto di una interrogazione parlamentare al ministro Rutelli (alla quale non sembra sia ancora arrivata risposta), in cui si esprimeva preoccupazione per la mancanza di "effettiva e concreta trasparenza nella predisposizione di atti normativi o para-normativi, nonché una partecipazione diretta aperta anche alle associazioni di utenti e cittadini" e del rischio che il sistema dei codici di autoregolamentazione "ispirati" dall'esecutivo "rischino di sottrarre o facilitare la sottrazione della podestà legislativa del Parlamento ." [17]

Si serve dello stesso metodo anche il Ministero delle comunicazioni che promosse (con l'on. Gasparri) la predisposizione del codice deontologico "Internet e minori" e nel quale si registrò il tentativo di far passare come "autoregolamentazione" l'adozione di sistemi per la verifica automatica dell'età di chi utilizzava determinati servizi e che presupponeva un articolato sistema di classificazione di contenuti - filtraggio della navigazione, insomma e potenziale schedatura. Cambiano le maggioranze, ma i metodi restano: siamo a luglio 2007 e il Ministero conferma in una intervista rilasciata al quotidiano La Repubblica che il "codice internet e minori" confluirà in una nuova "autoregolamentazione" chiamata "media e minori". "Vogliamo lavorare a braccetto con le aziende senza imposizioni" si legge in un occhiello dell'articolo [18]. Excusatio non petita, imputatio manifesta dicevano i latini. Fatto sta che circa un mese prima dell'articolo pubblicato da Repubblica, lo stesso Ministero delle comunicazioni aveva "caldamente suggerito" ai fornitori di accesso all'internet di rendere irraggiungibile dall'Italia un sito tedesco che ospitava contenuti - certo - semplicemente inaccettabili e vergognosi, ma la cui rimozione sarebbe eventualmente stata dovere della magistratura (nemmeno italiana, peraltro). Non certo di un "decreto orale" del Ministero. Un comportamento incredibile, degno delle peggiori teocrazie occidentali e medio-orientali, ma che è passato praticamente inosservato ancora una volta grazie all'associazione fra "Mr. Internet" e "i pedofili".

DATI PERSONALI E CODICI DEONTOLOGICI: UN'ALTRA FACCIA DEL PROBLEMA

Se "Patto di Sanremo" e "Media e minori" sono frutto di "attività" politiche, e sono privi, sulla carta almeno, di meccanismi sanzionatori seri, i "codici deontologici" previsti dalla disciplina sul trattamento dei dati personali sono contenuti in un decreto legislativo e quindi "devono" essere emanati. Inoltre, una volta entrati in vigore, diventano punto di riferimento per l'applicazione anche delle sanzioni penali previste dal Codice dei dati personali. Giornalisti, banche, assicurazioni, investigatori privati e anche "fornitori di servizi di comunicazione elettronica" sono letteralmente "obbligati ad autoregolamentarsi" con il Garante per la protezione dei dati personali che funge da semplice "notaio" e verifica che i codici non violino la legge. Nella realtà dei fatti, invece, il Garante gioca una parte attiva nella definizione dei contenuti dei codici in questione. E dunque il risultato finale non cambia: anche in questo caso le regole che dovrebbero essere spontaneamente definite da chi opera sul campo sono fortemente condizionate da un soggetto pubblicistico, per di più autonomo rispetto al Parlamento e all'Esecutivo.

CONCLUSIONI: VERSO LO STATO ETICO

Già a livello semantico il ricorso sistematico ed esagerato a termini quali "deontologia", "buona condotta" e "co-regolamentazione" evidenzia chiaramente l'orientamento di chi controlla il potere esecutivo e le altre "leve": stabilire autarchicamente cosa sia "buono" e "giusto" a prescindere dal diritto positivo e dal sistema del bilanciamento dei poteri caratteristico di uno Stato democratico. Quando si persegue un "fine superiore" non si può essere intralciati da qualche cavillo da leguleio, e se le norme non sono state scritte in modo abbastanza "flessibile", devono essere semplicemente ignorate. E in tutto questo "Mr. Internet" è soltanto la scusa per mettere mano a temi altrimenti intoccabili.

Almeno per un attimo, allora, proviamo ad elencare le questioni aperte e sottintese ogni volta che si parla di "Mr. Internet", ma senza far riferimento ad aspetti tecnologici:

- Perché lo Stato impedisce la libera circolazione di informazioni imponendo filtri e controlli immotivati?
- Perché lo Stato, utilizzando tecnologie costose, inutili e inefficienti costringe i cittadini a spendere di più (anche indirettamente, con le tasse) per usufruire di servizi pubblici che sono già "pagati" dal prelievo fiscale?
- Perché lo Stato consente di censurare contenuti senza che questo sia stabilito da una legge o da un magistrato?
- Perché lo Stato, invece di punire chi vìola effettivamente la legge, decide preventivamente "cosa è meglio" per ciascuno di noi?

Già... perché?

NOTE

[1] Pippo Battaglia rileva acutamente che la vera essenza della sindrome di Frankenstein, di assistere a quel che più temiamo: vedere una macchina divenire indipendente dal creatore. Battaglia, P. L'intelligenza artificiale. Dagli automi ai robot «intelligenti», Torino, 2006 p.3.

[2] Come la famigerata internet bubble che “vaporizzò” miliardi di dollari sui mercati borsistici di tutto il mondo. Vedi Livraghi, G. I postumi della bolla in Il mercante in rete n. 56 - http://gandalf.it/mercante/merca56.htm#heading01 e anche dello stesso autore Il potere della stupidità, Pescara II ed. 2007.

[3] Basta citare, fra tutti la vergognosa strumentalizzazione delle violenze sui minori. Un problema grave che è servito - con la legge 269/98 prima e con la “legge Prestigiacomo” poi - per ampliare i

poteri di polizia e imporre filtraggio di contenuti e schedature. Senza che, ovviamente, le vere vittime delle violenze, i minori abusati, siano stati effettivamente meglio tutelati.

[4] Atti del convegno "Internet: libertà e censura" CGIL Nazionale - Ufficio Nuovi Diritti Roma, 22 luglio 97 - http://www.cgil.it/org.diritti/internet/22LUGLIO/22LUGLI O.htm

[5] Peraltro, non è nemmeno detto che gli strumenti di controllo attualmente disponibili - internet compresa - siano necessariamente più efficienti o funzionali di quelli disponibili nel passato. Prima e durante la Guerra Fredda, le strutture di polizia politica dei due blocchi riuscivano benissimo a tenere sotto controllo “sospetti”, “simpatizzanti” e spie. Sui metodi praticati in Germania Est dalla STASI prima dell’avvento dell’informatica, vedi, per esempio, Wolf, M. Memoirs of a Spymaster Pimlico, 1998.

[6] Tanto per fare un esempio, il famigerato “419 scam” altresì noto come “Nigerian Scam” era ampiamente praticato anche prima della posta elettronica, sfruttando oltre all’ìmbecillità delle persone, fax e telefoni.

[7] Livraghi, G. Cassandra - http://gandalf.it/free/cass.htm

[8] Livraghi G. - Monti A. The Network Society as Seen From Italy in The Information Society 1 May 2002, vol. 18, no. 3, pp. 165-179.

[9] Indicativa, in questo senso, la vicenda legata alla diffusione del software open source e su cui si rinvia a ALCEI – È compito delle istituzioni pubbliche liberarci dalla schiavitù elettronica - http://www.alcei.it/?p=48

[10] È veramente indicativo, a tal proposito, il caso dell’esclusione di Furio Colombo dalla candidatura alla segreteria del nascituro Partito Democratico, che è stata possibile proprio grazie all’analfabetismo tecnologico del candidato e dei suoi sostenitori. Per quanto la motivazione del “comitato dei saggi” - i fax non sono sufficientemente “probanti” - sia giuridicamente sbagliata, se Colombo avesse chiesto di utilizzare quantomeno la firma digitale il problema della validità della sua candidatura non si sarebbe nemmeno posto. “it would have been entirely possible to run for the Democratc Party board by handling a digital electoral campaign. Why, then, Mr. Colombo didn’t use it? Complex answer for a simple question. The deadly mixture of legislator’s lack of

competence and Certification Entities wrongly aimed lobby efforts created a poisoned cocktail that almost killed the possibility to have these technologies at handy for the “average” citizen. BTW, nobody seemed really care to actually enhance the use of digital signature and certified e-mail through the citizenship.” così Monti, A. Italian Democratic Party’s Competition: faxes aren’t good enough to support a candidate in Digital Thought - http://blog.andreamonti.eu/?p=37

[11] Il caso più eclatante è sicuramente quello di Skype. Il fatto che - a differenza di altri sistemi VoIP - Skype offra gratuitamente dei veri e propri criptotelefoni software sta creando preoccupazioni e imbarazzi sia fra gli operatori (che vorrebbero poter “chiudere” le proprie reti al traffico di questo tipo perché non genera alcun utile e carica eccessivamente la banda passante a disposizione dei clienti), sia fra i poteri pubblici (preoccupati di non poter intercettare liberamente quello che circola in rete). Vedi anche sul punto Clarkson, A. Network Neutrality in ICTLEX BRIEFS n. 4/06 - http://www.ictlex.com

[12] Non che le imprese siano sempre e solo dei poveri succubi dei governi. Nel 2004 le grandi imprese IT cominciano a progettare l’implementazione su larga scala di sistemi di Digital Right Management a livello hardware con la scusa di “proteggere la proprietà intellettuale” ma contribuendo, in realtà, a creare mercati chiusi e problemi per gli utenti. Ecco il comunicato stampa dell’epoca: HP Announces Digital Entertainment Strategy with New Products and Partnerships Across Music, TV and Movies - http://www.hp.com/hpinfo/newsroom/press/2004/04010

Il prototipo di questa strategia manipolativa arriva dagli Stati Uniti13, ed è stata poi applicata - peggiorandola - anche in Italia. Fin dal 2005, grazie al discutibile credito attribuito a “statistiche”14 sui fenomeni illeciti commessi tramite l’internet a una malintesa interpretazione del concetto di “autoregolamentazione”, i ministeri dei beni culturali e delle comunicazioni stanno di fatto condizionando le imprese e i diritti degli utenti senza che il Parlamento possa - o voglia - minimamente intervenire. Come è noto l’autoregolamentazione - nota anche come “autodisciplina” - è una sorta di “trattato privato” che le aziende di un determinato settore decidono spontaneamente di predisporre e firmare.

Lo scopo dell’autodisciplina è quello di dare alle imprese delle regole comuni di comportamento, andando a colmare dei vuoti normativi o estendendo leggi più favorevoli anche a situazioni in cui questo si potrebbe evitare. L’autodisciplina, inoltre, serve a mettere a 8a.html - Comunicato stampa del 4 ottobre 2004 - Intellectual Property: As part of its overall digital entertainment strategy, HP is

taking a strong stance on protecting the intellectual property of artists and creators of content. Starting today, HP is stepping up its commitment to building, acquiring or licensing the best content protection technologies for HP devices that will set secure copyrights without sacrificing great consumer experiences - and will strive to build every one of its consumer devices to respect digital rights. For example, HP will build support for a technology called Broadcast Flag into its TVs, media hubs and Media Center PCs in products rolled out after June. The Broadcast Flag signals that the content must be protected and cannot be shared indiscriminately over the Internet. The technology does not prevent consumers from making multiple copies of digital content and sharing it within a home network or storing it on physical media such as DVDs.

Nel 2005 ha suscitato molto rumore il caso Sony-BMG, in cui l'azienda ha utilizzato un software potenzialmente pericolo per proteggere i CD musicali dei quali detiene i diritti, senza avvisare gli utenti della sua esistenza. Vedi Nella frenesia dei tentativi di impedire la riproduzione di musica, la Sony BMG Entertainement diffonde software pericolosi http://www.alcei.it/?p=106

[13] Nel 2004 da Adobe che su richiesta delle istituzioni finanziarie americane aveva incorporato in Photoshop dei sistemi anticontraffazione di cui gli utenti - trattati loro malgrado da potenziali falsari - erano stati tenuti all'oscuro. Vedi Bridis, T. Adobe Says It Uses Anti-Counterfeiting Technology in The Washington Post E.03 - 10 gennaio 2004. "Experts said the decision by Adobe represents one of the rare occasions when the U.S. technology industry has agreed to include third-party software code into commercial products at the request of government and finance officials." e il messaggio pubblicato sul forum degli utenti Adobe che segnalava il problema http://www.adobeforums.com/cgibin/ webx?13@215.1oTzbbQUVVh.0@.2ccf3d27

[14] Sull'abuso delle statistiche vedi Huff, D. How To Lie With Statistics ed. it. Mentire con le statistiche Pescara, 2007 e ibidem nelle aggiunte all'edizione italiana per alcune analisi dedicate specificamente ai mezzi di comunicazione.

[15] Il caso delle problematiche connesse alla gestione dei nomi a dominio del ccTLD .it. è emblematico del disinteresse politico verso temi critici ma scomodi e non "alla moda". Per anni - e in parte ancora oggi - le strutture pubbliche del CNR sulle quali si appoggia il Registro del ccTLD.it sono state gestite in violazione di legge (basta pensare al mancato rispetto della disciplina sul trattamento dei dati personali in rapporto al Whois).

Nonostante il fatto fosse ampiamente noto, il Garante dei dati personali non ha mai adottato alcun provvedimento. Nel 2000 solo all'indomani della registrazione da parte di terzi di alcuni nomi a dominio di illustri politici, il governo - nella persona del senatore diessino Stefano Passigli si affrettò a presentare un disegno di legge inutile e confuso al quale nessuno diede - fortunatamente - seguito. Nello stesso tempo, però, nessun governo (passato e presente) ha mai voluto seriamente occuparsi dei gravi problemi legati alla gestione del Registro italiano.

[16] Cammarata, M. Utenti canzonati nel patto della canzonetta in Interlex del 7 marzo 2005 - http://www.interlex.it/copyright/sanremo.htm

[17] Interrogazione Acerbo-Folena del 20 giugno 2006 a risposta scritta al Ministro dei beni culturali http://www.interlex.it/copyright/interr_patto.htm

[18] Vedi Longo, A Minori, arriva un codice per tutti i media in La Repubblica del 22 luglio 2007 p. 22

ALESSANDRO NICOTRA

Tecnica, diritto, formazione e modelli collaborativi

Alessandro Nicotra, milanese, laureato in giurisprudenza, consigliere di Isoc Italia ha rappresentato l'associazione al WSIS di Tunisi. Specializzato in nuove tecnologie e diritto informatico, impegnato in Internet dal 1994 ha recentemente fondato le associazioni Italia Digitale e Diritti Digitali che ha l'onore di presiedere. Con la creazione del primo gruppo di discussione di "cultura e religione" ha contribuito alla crescita della Usenet italiana. Collabora con la Cattedra di Informatica Giuridica dell'Università degli Studi di Milano e più diffusamente con diverse associazioni ed istituzioni accademiche e non. Promotore e responsabile di numerosi progetti nel campo della comunicazione, della formazione e dei processi di innovazione tecnologica. Curatore ed autore della rubrica Internet pubblicata dal mensile "Il Timone", promuove e partecipa attivamente a convegni ed eventi volti alla diffusione positiva della cultura Internet. Particolarmente attento al sociale ed al terzo settore studia modelli di sviluppo, modelli di regole e modelli economico-formativi, basati sulla collaborazione, sulla condivisione, sull'e-learning e sul software Floss.

Per anni Internet è riuscita a progredire grazie a Gentlemen's Agreements ovvero grazie ad un protocollo comportamentale basato su correttezza ed efficienza: un modus operandi non scritto ma vigente fra tutti i tecnici, gli scienziati, gli accademici e gli esperti del settore. Gli unici protocolli formalizzati, attraverso le cd. RFC [1], diventavano e diventano così delle "Leggi"di riferimento con un'unica ma efficace sanzione, in caso di mancato rispetto o di mancata adozione, per quanti costruivano ed usavano la Rete: l'esclusione e l'emarginazione di fatto.

Del resto, che senso avrebbe, una volta convenute a livello internazionale delle unità di misura, adottarne di nuove che non permettano l'interoperabilità tra sistemi, la conversione e lo scambio di dati, di merci o di altra qualsivoglia relazione e correlazione? Non è forse l'uomo un animale necessariamente sociale? L'enorme, e parzialmente inaspettato, successo dell'Internet si è avuto proprio grazie a questi protocolli aperti e condivisi che hanno reso antieconomico ed irragionevole mantenere sistemi e modelli proprietari che non possono o non riescono a comunicare ed operare tra loro. Necessità e concetti, questi, da tempo noti a quanti si occupano di scienza, di cultura, ma anche a quanti si occupano di infrastrutture, di commercio e di diritto internazionali.

Quanto appena descritto, se da un lato può sembrare una ricostruzione superficiale o faziosa o peggio ancora una ingenua e semplicistica analisi di quella che è stata ed è una rivoluzione di fatto, dall'altro fu proprio, in estrema sintesi, quanto si verificò a partire dagli anni '90, quando il mercato, da sempre attento ai numeri, ritenne opportuno adottare e promuovere il già diffusissimo Internet Protocol Suite ovvero quell'architettura di rete, basata su protocolli come il TCP/IP, creata da Robert Kahn e Vinton Cerf anni addietro e, successivamente implementata, tramite le già ricordate RFC, dalla comunità internazionale dei tecnici e degli esperti, che costruivano ed usavano materialmente quelle reti. Una anomalia resa ancor più evidente dal fatto che in realtà esisteva anche un protocollo OSI (Open System Interconnection) voluto nel 1979 dal più importante ente di standardizzazione internazionale, l'ISO [2], e definito "dall'alto" come standard per le reti di telecomunicazioni mondiali, ma poi abbandonato per ragioni pratiche.

Con il riconoscimento alquanto interessato, infatti, da parte del mercato si assistette al successo di una serie di protocolli scaturiti da un nuovo modello culturale, fondato sulla collaborazione tra società civile, laboratori di ricerca ed università, sui formati aperti, sulla individuazione di soluzioni funzionali e neutrali piuttosto che finalizzate a capricci ideologici o ad interessi esclusivamente economici di uno o più persone, istituzioni o gruppi di potere. Si realizza, quindi, una anomalia di storica portata che non sovverte ma semplicemente si affianca ed offre, per la formazione la produzione e l'adozione di standards, un percorso alternativo a quello classico dato soprattutto dall'intreccio tra politica e poteri forti. Mentre l'approccio "classico" cerca di imporre o far adottare "dall'alto" (top to the bottom) determinati standard, convenzioni e regole, rivendicando un potere d'indirizzo basato più o meno apertamente sul principio di autorità e diffuso tramite un uso strumentale (con esiti non sempre ottimali quando non, addirittura iniqui) delle legislazioni sovranazionali o locali, il "nuovo" metodo ed il modello operativo tecnico, quale è quello delle RFC e di ISOC, si sviluppa e si diffonde "dal basso" (bottom to the level), da parte degli stessi attori della rivoluzione informatica e su basi prettamente funzionali, arrivando ad imporsi per diffusione virale e volontaria, con un'adozione spontanea e di fatto, non per una qualche imposizione normativa o politica. I curiosi, gli storici, gli appassionati, ma soprattutto i critici e gli scettici, possono studiare e scoprire da soli numerosissimi aneddoti, interpretazioni e ricostruzioni sulla storia del modello collaborativo che caratterizzò e caratterizza l'operato dei pionieri dell'Internet, della IETF [3], dell'ISOC [4] e dei gruppi di lavoro speculari. Quello che si vuole qui rivendicare ed oggettivare, invece, è quel normale e giustificabile sentimento di orgoglio e di appartenenza a questa comunità "Internet" che ha contraddistinto e contraddistingue tutti coloro che vi

contribuirono e vi parteciparono "in solido" quando non era ancora un fenomeno di massa e non ci si sognava nemmeno di brandire il diritto per querele, denunce od azioni penali.

Il fenomeno informatico era, sino a vent'anni fa, ancora riservato a ristretti gruppi di accademici, di tecnici o di inguaribili appassionati di nuove tecnologie. Quel mondo caoticamente ordinato ed ispirato ad una sana competizione volta a primeggiare in conoscenza ed in capacità visionarie-esplorative, oggi, è stato in qualche modo stravolto dalla diffusione dei personal computer, dall'irrefrenabile ed esponenziale crescita delle connessioni tra questi o tra questi ed i nuovi dispositivi mobili e proprio dal successo di una così diffusa ed aperta distribuzione od accessibilità dell'informazione e al "potere" di contribuirvi personalmente. Invero, l'aumentare degli utenti aveva comportato dei primi esperimenti di autoregolamentazione sociale e non più meramente tecnica sul come ci si dovesse comportare ed interfacciare sul Web: nacquero i primi tentativi di autoregolamentazione come la Netiquette, apparvero i moderatori nei gruppi di discussione e via discorrendo. Ciò nonostante, si è arrivati al paradosso di criticare ed indicare come punti deboli ed accusare proprio quegli aspetti tecnico-sociali della Rete che ne hanno determinato la diffusione a livello planetario (e prossimamente interplanetario [5]): l'apertura dei protocolli, l'architettura agnostica e determinate sue implementazioni tecniche, necessariamente e funzionalmente neutrali. Si è arrivati a confondere causa ed effetti, mezzi e fini, infrastruttura e punti terminali, protocolli di trasporto dei dati con il contenuto dei dati stessi. Sul punto, Isoc Italia ha già pubblicato in passato un Quaderno dedicato alle c.d. Patologie della Rete, illustrando come Internet sia e rimanga uno specchio della società, nel bene e nel male. L'ignoranza, la povertà, la maleducazione, i truffatori, i ladri, i pedofili... Sono tutti aspetti della vita reale e della società umana, non peculiarità imputabili all'esistenza della Rete che si limita, semmai, a farli emerge in tutta la loro crudezza, costringendoci ad affrontarli ed anzi, dandoci spesso una opportunità in più per poterlo fare.

Internet non ha mutato o trasformato l'essenza delle cose e della realtà. Sino a qualche hanno fa certi "guru" (più del marketing che delle cose della vita invero) solevano parlare del mondo digitale come di un mondo virtuale e, quindi, non esistente se non metafisicamente, come i sogni od i pensieri. Una cantonata, questa, che potevano prendere e far prendere solo quanti non avessero fatto esperienza vera e diretta di quel mondo e di cosa implicasse il connettersi ed il connettere in Rete. La nuova società dell'Informazione, il nuovo mondo digitale non è meno virtuale di un quadro, di un disegno, di un componimento letterario musicale o di una scenografia: tutte queste cose non sono altro che forme di rappresentazione della realtà. L'aspetto veramente rivoluzionario dato dalla rappresentazione binaria della vita in bit, bytes e data packets è dato dalla nuova dimensione

creatasi e da una nuova, non meglio definita e definibile, percezione spazio-logico-temporale che si è venuta a creare con l'Internet. Basti pensare alla scomparsa dei confini tradizionali ed ai conseguenti problemi di giurisdizione, ma si pensi anche alla scomparsa di valenza tra originale e copia di un bene immateriale (libro, fotografia o canzone per intenderci) una volta riversato in formato digitale. Si pensi al paradosso della protezione dei dati personali, intimamente e necessariamente correlati alla propria identità digitale ovvero della propria identità in Rete, cui si contrappone l'aspirazione ed il diritto a più identità, fittizie ma con implicazioni reali, come nel gioco on line Second Life. Per sottacere, poi, sugli altrettanti e paradossali effetti dati dalla voglia di sempre più individui di mettersi in mostra rectius di comunicare e di conoscere, cui non corrisponde altrettanta voglia di capire e di approfondire le implicazioni connesse all'uso delle nuove tecnologie. Ed ancora, si pensi, infine, all'eccesso di informazione disponibile e, per contro, alle capacità umanamente limitate di vagliarla tutta od almeno una piccola parte in modo critico, cosa, quest'ultima, che finisce col tributare o innestare nella Rete anche un'anima o una parascientifica forma di anelito spirituale e/o di religiosità (Chi siamo? Da dove veniamo? Cosa è vero e cosa è giusto? E soprattutto, quale tortura, - per contrappasso - infliggere allo spammer che ci ha intasato l'email?).

Insomma, l'Internet come dimensione dove tutto e il contrario di tutto viaggiano fittamente intrecciati, a velocità sempre più elevate, lasciando agli individui ed agli utenti finali di vagliare e di setacciare cosa sia per loro, per loro solo e per il loro solo e proprio computer/terminale/punto/nodo di rete: buono o cattivo, giusto o sbagliato, legale o illegale, opportuno o inopportuno. Dal punto di vista storico, filosofico e sociologico, i detrattori amanti delle definizioni e delle "rassicuranti" categorizzazioni hanno buon gioco a confondere la causa con gli effetti, quando analizzano il fenomeno dell'Internet, arrivando addirittura a definire e bollare certe manifestazioni-rappresentazioni non come aneliti e conseguenze della natura umana (quali possono essere la curiosità, la libertà e la conoscenza) bensì come espressioni di "insopportabile" ed intollerabile anarchia. Per costoro, infatti, sembrerebbero concretamente "materializzarsi", attraverso la Rete, le idee e le utopie di quella mutua cooperazione teorizzata da Pierre-Joseph Proudhon [6] e di quella rivoluzione teorizzata da Michail Aleksandrovi? Bakunin [7] con lo Stato, il capitale e la borghesia mondiali attaccati e messi sotto assedio da un proletariato agguerrito, informatizzato ed autogestito.
Al di là di un più o meno dotto e anacronistico tentativo di ricondurre all'attualità od adattare categorie di pensiero e di linguaggio che appartengono ormai al passato millennio, è innegabile, invero, che gli informatici ed i tecnici siano sempre stati abbastanza allergici a qualsivoglia codifica che non fosse segnatamente ed esclusivamente hardware o software. Ma non certo per motivi

ideologici quanto piuttosto per la natura ed il crogiolo stesso dove ha iniziato a formarsi ed evolversi il nuovo mondo digitale. Un crogiolo ed un ambiente dove il diritto e le norme giuridiche erano corpi estranei e non pertinenti alla scoperta di innovativi sistemi e sinapsi elettroniche, anzi erano percepiti come certa scienza percepisce la fede e la religione ovvero come degli ostacoli all'esplorazione stessa. Paradigmatica, in tal senso, la connotazione ed il diverso significato che ha assunto in un lasso di tempo insolitamente breve il termine Hacker [8]. Quanto costruito e posto a fondamento della odierna società dell'Informazione dai Cerf, dai Kahn, dai Postel, dai Berners-Lee, dalle RFC e dai "gentil uomini" tutti, oggi è diventato anziché fonte di vanto e di progresso, una fonte di manzoniane grida di dolore sull'assenza di regole e via scandalizzando. Viene invocato da più parti un maggior controllo ed una diversa gestione nazionale ed internazionale, viene organizzato il WSIS ed i successivi Forum mondiali sull'Internet governance, attorno ai quali vengono agitati, accanto agli abusati spettri dei virus e dello spam, quelli della pedofilia, dei furti di identità digitale, della privacy, della sicurezza e di ogni sorta di diritto violato. Ironicamente, si potrebbe osservare e sintetizzare che l'Internet da attrattore strano [9] e sano della Teoria del Caos sembrerebbe essere regredito a causa della sua crescita indiscriminata e vertiginosa nel più classico e greve casino dato dalla Pratica umana.

Tutto torna. Quello di Internet sarebbe un modello anarchico di esaltazione della libertà e come tale utopico, dannoso e bisognoso di governo e di controllo da parte degli stati.... La tentazione, una pessima tentazione, cui molti han già ceduto, è quella di lasciar dire e fare alla politica ed a certi potentati che "tanto noi si va per la nostra strada". A colpi di realpolitik (come il contentino dato all'AAMS italiana per censurare i siti di scommesse on line non autorizzate), di strappi tecnocratici e strilli ideologici, si finisce per regredire davvero e si riprende a parlare linguaggi diversi senza cogliere in tutta la loro evidenza i veri rischi involutivi cui la nuova società dell'Informazione va incontro. Per quanti pruriti e crisi di orticaria possa provocare, è giunto il momento che i tecnici interagiscano in modo meno presuntuoso e più collaborativo con certi giuristi; ed è giunto il momento che i giuristi si facciano carico di proposte equilibrate per mantenere la neutralità e le potenzialità di sviluppo della Rete, rintuzzando le capziose motivazioni addotte da certi governi, da certe organizzazioni e da alcune multinazionali che vedrebbero volentieri il ritorno a vecchi sistemi economici, giuridici e sociali reintroducendo e diffondendo delle sotto reti chiuse e proprietarie (nelle quali è più facile intrappolare e tenere il proprio "parco buoi"), il controllo degli accessi, il ritorno ad una informazione intesa e gestita come potere da concentrare nelle mani di pochi e, più in generale, imponendo alla società globale il ritorno ad una cultura come privilegio ed appannaggio esclusivo degli abbienti e di chi può...

Un agguerrito zoccolo duro di pionieri dell'Internet, di loro eredi e di appassionati discenti, si è da tempo coagulato nell'ISOC, con l'intento di promuovere positivamente e attivamente la Rete, contribuendo ad affrontarne i problemi, ma anche con il tenace proposito di non vederla snaturata e sottratta alla collettività tutta. Accanto a questi, innumerevoli altre associazioni di ogni ordine e grado si sono preoccupate e interessate a che l'Internet continui a svilupparsi "dal basso", rimanendo lo straordinario veicolo di conoscenza, di progresso e di diffusione od accessibilità dell'informazione che è stato sinora. Ciò nonostante, quella che in altre circostanze è sicuramente un punto di forza, ovvero la diversità e la pluralità di voci, in questa fase di delicata transizione si sta evidenziando come pericoloso limite per l'incapacità o indolenza ed insofferenza di formalizzare proposte unitarie e di non disperdere le energie in migliaia di rivoli ed iniziative diverse. Ed è curioso osservare come si cerchi di delegittimare o tendere diplomatici tranelli proprio a quelle persone che la Rete l'hanno costruita, implementata, vissuta e voluta appassionatamente. Il riferimento, sia detto in modo ancora più esplicito, è a quel divide et impera cui tentano di giocare i centri di interesse e di potere politico-economici, sia a livello nazionale che internazionale, usurando pionieri, veterani, proseliti e veri appassionati dell'Internet in una battaglia difensiva ed in continue e sfibranti mediazioni al ribasso.

Non è questo il luogo per un trattato comparativo tra giusnaturalismo [10], positivismo giuridico, formazione dei protocolli di Rete tramite RFC, governance e government. Questa libera dissertazione rappresenta piuttosto un accorato appello sui passi avanti che servirebbero. Servono infatti nuove regole condivise, serve un organico corpus di consuetudini del diritto informatico e della Rete, serve un approccio interdisciplinare e multidisciplinare che non esuli dal funzionamento tecnico e dai protocolli ma che, piuttosto, lo supporti e lo integri. Serve, per esempio, che i tecnici non pretendano di dare lezioni od imporre ai giuristi personali e fantasiose interpretazioni circa il diritto o la giurisdizione e serve che i giuristi non pretendano di stabilire quale sia il corretto funzionamento della Rete imponendo strumentali alterazioni al DNS. Serve, più d'ogni altra cosa, lasciare fuori ogni strumentalizzazione ed ideologia per capirsi a prescindere dagli argomenti, siano essi economici politici legali sociali culturali o tecnico-scientifici, arrivando a concordare ed a redigere le XII tavole [11] dell'Internet. Quella attuale, per alcuni versi, ricorda una situazione speculare a quando i primi elaboratori non riuscivano a comunicare tra loro poiché ciascuno di essi aveva i rispettivi linguaggi macchina, hardware e sistema operativo. Se l'avvento in sordina e la diffusione del TCP/IP riuscì nel miracolo accertato di allora, possiamo ritenere non solo auspicabile, ma possibile, che questo miracolo di interoperabilità (o interdisciplinarietà, a seconda

degli interlocutori) si verifichi anche in questo momento storico ed epocale in cui l'Internet di massa richiede fortemente l'apporto ed il contributo di giuristi specializzati e di norme che sanzionino gli abusi della libertà piuttosto che il suo legittimo anelito.

Molti non comprendono che abdicare ad un qualsivoglia intervento normativo significa rimetterlo all'arbitrio di legislatori ignoranti e di una classe politica impreparata. Viceversa, adoperando lo stesso modello collaborativo che è alla base della creazione, della diffusione e della libertà dell'Internet, potrebbe essere possibile partecipare ad una formazione consapevole e non imposta di norme che siano soprattutto di tutela, di promozione e non di affossamento di questa nuova era digitale. In quest'ottica, un passaggio importante ed obbligato, che non potrà essere ignorato in sede di discussione all'Internet governance Forum che si tiene a Rio de Janeiro dal 12 al 15 novembre 2007, è quello della formazione. Spesso e giustamente si è richiamata l'attenzione al problema del Digital Divide e delle diversità linguistico-culturali, ma altrettanto importante e propedeutico alla soluzione di detti problemi è l'educare e l'introdurre, a partire dalle scuole occidentali prima ancora che da quelle dei c.d. Paesi in via di sviluppo, ai preponderanti vantaggi dati dai modelli collaborativi e cooperativi. Non è un caso, infatti, se L'Unione Europea al suo VII Programma Quadro [12] (valido per il quinquennio 2007-2013) ha dato il titolo "Costruire l'Europa della conoscenza", varando quattro programmi fra cui il primo e più importante è dedicato alla cooperazione. Allo stesso modo non è un caso che nel contributo che state leggendo si siano voluti privilegiare, nelle note a piè di pagina, i riferimenti ed i collegamenti a Wikipedia, la celebre enciclopedia formatasi liberamente grazie alla collaborazione di milioni di persone in tutto il mondo. Sul fronte della formazione, inoltre, si gioca anche la concreta possibilità di varare e soprattutto di diffondere e far rispettare, a livello mondiale, una sorta di Carta dei Diritti Digitali [13] oltre che dei Diritti dell'Internet. Poiché non vi è libertà senza conoscenza e consapevolezza, non vi potrà essere una diffusa adozione e rispetto di quei valori e di quei principi che sono già in un qualche modo espressi nella Carta dei Diritti dell'Uomo, ma che necessitano di una rivisitazione e di una specifica contestualizzazione per essere applicati alla e nella Rete.

L'attuale momento storico, che lo si creda o no, è di quelli epocali ed in Italia (ma non solo in Italia) lo si avverte particolarmente quando si osserva il grave stato di crisi in cui versano la politica, il diritto e l'economia. Chi scrive, non pensa che il Re sia stato messo a nudo, ma anzi che ad essere messo a nudo (per colpa o per merito anche e soprattutto della società Internet) sia stato l'individuo, l'uomo occidentale, il bisogno, il disperato bisogno di tornare a relazionarsi, ad interagire e decidere per interessi meno egoistici e contingenti, di costruire qualcosa e ridare un senso al nostro vivere

terreno. Si parla da più parte delle crisi occidentali: economica, morale, sociale e financo d'identità (con le oggettive radici giudaico-cristiane che diventano un concetto troppo "forte" per essere affermato). Ed allora, perché quest'era digitale possa trasformarsi in un'era di vero e diffuso progresso è indispensabile "ripartire" investendo sulla formazione e sulla inculturazione, una educazione informatica, intrecciata alla dimenticata educazione civica, come base, come opzione concreta per arrivare a scelte, in un futuro prossimo e specie nell'ambito delle nuove tecnologie, che siano consapevoli, adottate spontaneamente per convinta diffusione e non per mera imposizione normativa. Fantascienza? Scenario limitabile esclusivamente a piccole comunità di Padri Pellegrini [14] ?

Prevenendo facili ironie o critiche materialistiche, l'invito è ad interrogarsi sul perché un numero decisamente rilevante di persone in tutto il mondo abbiano contribuito e continuino a riempire gratuitamente il web di contenuti, propri e non. Per lo stesso motivo, nel tentativo di spiegare certi fenomeni, antichi e nati ben prima che qualche furbetto del marketing li brevettasse come Web 2.0 o qualche manager/giornalista rampante se ne servisse con odiate etichette tipo folksonomy e social engineering, e nel tentativo di illustrare, in conclusione, perché l'Internet deve rimane neutrale, deve rimanere libera, ma deve anche darsi delle regole giuridiche oltre che tecniche, si preferisce riportare qui le più autorevoli riflessioni di Immanuel Kant nella sua 'Critica della Ragion Pratica':

"Due cose riempono l'animo con sempre nuovo e crescente stupore e venerazione, quanto più spesso e accuratamente la riflessione se ne occupa: il cielo stellato sopra di me, e la legge morale in me. Entrambe le cose non posso cercarle e semplicemente supporle come fossero nascoste nell'oscurità o nel trascendente, al di fuori del mio orizzonte; io le vedo davanti a me e le collego immediatamente con la coscienza della mia esistenza. Il primo comincia dal luogo che io occupo nel mondo sensibile esterno, ed estende la connessione in cui mi trovo nell'infinitamente grande, con mondi sopra mondi e sistemi di sistemi, e inoltre nei tempi illimitati del loro movimento periodico, nel loro inizio e nella loro continuità. La seconda comincia dalla mia invisibile identità, la personalità, e mi pone in un mondo che possiede vera infinità, ma di cui si può accorgere solo l'intelletto, e con il quale (ma grazie ad esso anche con tutti quei mondi visibili) io non mi riconosco, come là, in una connessione puramente accidentale, ma in una necessaria e universale. Il primo sguardo di una innumerabile quantità di mondi per così dire annienta la mia importanza, che è quella di una creatura animale, che dovrà restituire ai pianeti la materia da cui è sorta, dopo essere stata dotata per breve tempo (non si sa come) di forza vitale. Il secondo al contrario innalza infinitamente il mio valore, che è quello di una intelligenza, grazie alla mia personalità, nella quale

la legge morale mi rivela una vita indipendente dall'animalità e anche dall'intero mondo sensibile, perlomeno quanto può essere dedotto dalla destinazione finale della mia esistenza attraverso questa legge, che non è limitata alla condizioni e ai confini di questa vita, ma si estende all'infinito. Però, stupore e rispetto possono sì spingere alla ricerca, ma non sostituirne la mancanza . ..." [15].

NOTE

[1] RFC ovvero “Request for comment”. Per saperne di più è possibile consultare il seguente documento in inglese: “The Internet Standards Process -- Revision 3” (http://www.ietf.org/rfc/rfc2026.txt) o la voce italiana “RFC” su “Wikipedia” (http://it.wikipedia.org/wiki/Request_for_Comments.

[2] L'International Organization for Standardization (http://www.iso.org).

[3] L'Internet Engineering Task Force (http://www.ietf.org/overview.html).

[4] Si tratta dell'Internet SOCiety fondata e voluta da Vinton Cerf e da molti padri fondatori dell'Internet (http://www.isoc.org).

[5] Si veda l'Interplanetary Internet Project: http://www.ipnsig.org/

[6] Conosciuto come il primo filosofo e politico definitosi anarchico, Proudhon sosteneva l'urgenza di realizzare una società senza autorità, perché nel principio di autorità sarebbe insito quello di sfruttamento.

[7] Considerato uno dei padri fondatori dell'anarchismo moderno (http://it.wikipedia.org/wiki/Michail_Bakunin)

[8] Vedasi la dettagliata e corrispondente voce su wikipedia al link: http://it.wikipedia.org/wiki/Hacker

[9] Concetto matematico che indica un insieme verso il quale evolve un sistema dinamico dopo un tempo sufficientemente lungo (http://it.wikipedia.org/wiki/Attrattore_strano).

[10] http://it.wikipedia.org/wiki/Diritto_naturale

[11] http://it.wikipedia.org/wiki/XII_tavole

[12] http://europa.eu/scadplus/leg/it/lvb/i23022.htm 13 Nel tentativo di studiare e stimolare i migliori contributi è stata costituita, nel corso del 2007, in Italia una nuova associazione, impostata come Working Group giuridico e denominata appunto Diritti Digitali (http://www.dirdig.org) che ambisce a proporre un approccio innovativo e soluzioni giuridiche più eque in questo ambito che ha ed avrà un crescente peso nella vita delle persone. 14 I Padri Pellegrini vengono tradizionalmente considerati i

[13] Nel tentativo di studiare e stimolare i migliori contributi è stata costituita, nel corso del 2007, in Italia una nuova associazione, impostata come Working Group giuridico e denominata appunto Diritti Digitali (http://www.dirdig.org) che ambisce a proporre un approccio innovativo e soluzioni giuridiche più eque in questo ambito che ha ed avrà un crescente peso nella vita delle persone.

[14] I Padri Pellegrini vengono tradizionalmente considerati i primi coloni del Nuovo Mondo (http://it.wikipedia.org/wiki/Padri_Pellegrini)

[15] Tratto dalla Ragione pratica, A 287-290, di Immanuel Kant.

TULLIO PADOVANI

Tutela della riservatezza e internet: un binomio difficile. Il caso delle intercettazioni delle comunicazioni informatiche o telematiche.

Tullio Padovani, nato a Udine il 27 marzo 1944. Assistente ordinario di diritto penale presso la Facoltà di giurisprudenza dell'Università di Pisa dal 1965. Nel 1973 professore incaricato di diritto penale e dal 1980 professore ordinario di diritto penale presso la medesima Facoltà. Dal 1988 professore ordinario di diritto penale presso la Scuola Superiore "S. Anna" di Pisa. è autore di numerosi saggi e monografie, oltre che di un manuale di diritto penale giunto all'ottava edizione. Coordina i Commentari Giuffrè al Codice penale e alla Legislazione penale complementare. Condirige le riviste "La legislazione penale" e "Rivista Italiana di Diritto e Procedura Penale". Ha fatto parte di numerose commissioni presso il Ministero della giustizia, tra cui quelle per la riforma del codice penale presiedute da Pagliaro, Nordio e Pisapia.

L'innesto dei mezzi informatici in tutti i centri vitali della società moderna, dal sistema sanitario al sistema bancario, da quello delle telecomunicazioni al sistema commerciale da quello scolastico a quello della difesa, fino all'uso più strettamente "domestico" del computer e di internet ha inciso notevolmente sulla tutela della riservatezza latu sensu intesa.

Da una parte, in effetti, ogni volta che decidiamo di accendere il computer e accedere ad Internet per compiere una qualunque operazione siamo invasi, tecnologicamente parlando, e senza esserne affatto consapevoli, da programmi e programmini che carpiscono informazioni su di noi (sui siti che visitiamo, sul tempo che vi sostiamo, sul percorso che vi compiamo, sul luogo dal quale lavoriamo ect.), e che poi sono in grado di inviare al loro produttore, ma anche di immagazzinarle, rielaborarle e recuperarle ad ogni nostro successivo accesso ad Internet od a quello specifico sito, tanto che possiedono una memoria storica della nostra vita nelle rete (si tratta, in particolare, dei cookies, piccoli file che immagazzinano informazioni, e di programmi "spyware", vere e proprie neospie tecnologiche della nostra privacy).

Dall'altra, appena usciamo di casa, pressoché ogni nostro movimento è governato da un meccanismo informatico che ci coadiuva nelle più disparate attività, dall'acquisto del latte al supermercato con il bancomat, alla telefonata di lavoro con il telefonino, fino alla visita ospedaliera, nel quale lasciamo traccia del nostro passaggio.

Si tratta, invero, di una rivoluzione del modo di vivere positiva, se si pone a mente al fatto che era inimmaginabile fino a qualche tempo fa poter anche solo pensare di scambiare infinite informazioni in tutto il mondo nel giro di frazioni di secondo, tanto che, oggi, una scoperta effettuata nel posto più disparato della terra, una volta messa in Rete, diviene patrimonio di tutta l'umanità. Ma, al contempo, presenta anche rovescio della medaglia se taluno si propone di far un uso distorto di questo patrimonio immenso di informazioni sulle cose e sulle persone.

In particolare, le informazioni sulle cose hanno il loro risvolto negativo là dove su Internet, oltre alle ricette per un gustoso piatto straniero, si rinvengono anche le ricette per confezionare ordigni esplosivi, o informazioni pedopornografiche e via dicendo; mentre le informazioni sulle persone presentano il loro lato negativo nella possibilità, incrociando i dati immagazzinati ad ogni nostro spostamento sulla Rete o ad ogni nostro utilizzo di una qualche tecnologia, di effettuare un profilo dell'utente pressoché completo, con una inaccettabile invasione della privacy impensabile fino a qualche anno fa. D'altronde, prima della rivoluzione informatica, i pochi dati raccolti in occasione dell'acquisto di una casa o, ad esempio, di un ricovero ospedaliero, finivano poi in cartelle riposte in archivi polverosi e non sempre ben organizzati, tali da dissuadere dalla ricerca di informazioni il più solerte degli investigatori o dei venditori porta a porta.

La prospettiva è certo inquietante. Tale è la capacità di controllo sui singoli e di annientamento dell'anonimato oggi garantita dai sistemi informatici, che, in pochi secondi, è possibile sapere praticamente tutto di una persona, dalla sua età fino sue più strette abitudini di vita, tanto che, a paragone, fa quasi sorridere l'immagine del vecchio Grande Fratello di George Orwell, che appare oggi poco più di una innocente osservazione dal buco della serratura.

Una adeguata tutela della privacy è resa inoltre ancor più urgente dal fatto che la sua regolare violazione non è opera esclusiva delle società commerciali, o di chi lavora per esse a fini statistici o di promozione di servizi o per pubblicità personalizzate, ma anche e soprattutto dei governi e delle intelligences internazionali che si servono dei moderni mezzi tecnologici per la raccolta di informazioni su tutti, in funzione di controllo e prevenzione dalle aggressioni terroristiche, ma non necessariamente solo per quelle.

Una violazione della privacy, in conclusione, insidiosa perché sostanzialmente occulta, ma pervasiva e continua che ci cinge la vita privandoci di un diritto fondamentale, qual è appunto diritto alla riservatezza.

La tutela della riservatezza è un principio cardine di una società che voglia definirsi libera in senso sostanziale, e nel nostro ordinamento è tutelata, come è noto, dall'art. 15 della Costituzione, che riconosce il principio della inviolabilità della persona umana e sancisce espressamente la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione. Un diritto "naturale", si potrebbe dire, che ogni individuo ha, di decidere liberamente e senza controlli, che cosa condividere con gli altri, quando e quanto.

Tale bene giuridico trova tutela anche nell'ordinamento penale che si preoccupa di tutelare la segretezza e la libertà della vita del singolo nel suo domicilio nella sez. IV, del titolo XII, del libro II, del codice penale ("Dei delitti contro l'inviolabilità del domicilio"), e nelle sue comunicazioni, sez. V, del titolo XII, del libro II, del codice penale ("dei delitti contro l'inviolabilità dei segreti").

Tali classiche aggressioni alla riservatezza sono state oggetto di "ammodernamento" da parte del legislatore nel 1993. A ben vedere, infatti, le aggressioni tipizzate in epoca pre-tecnologica erano palesemente inadeguate rispetto alle nuove condotte aggressive che correvano lungo i fili telematici, tanto da dover prevedere nuove ipotesi di reato.

Particolarmente interessanti in proposito risultano le fattispecie poste a tutela delle comunicazioni. In effetti, insidioso è l'uso del mezzo informatico nell'intercettare le comunicazioni, perché, come si è detto, l'informatica, da una parte, facilita notevolmente tale modalità aggressiva, che non necessita più di particolari strumentazioni, ma solo di un computer e di una persona in grado di superare le poche barriere tecnologiche, e, dall'altra, ne aggrava notevolmente la capacità di penetrazione, vista la vastità della diffusione dei computer in rete e la rapidità di propagazione delle informazioni.

In altre parole, non vi è dubbio che il diritto penale riconosca come bene giuridico meritevole di tutela la segretezza delle comunicazioni; tuttavia, ciò che vi è di nuovo è l'insidiosità delle nuove aggressioni non solo quantitativamente, ma anche qualitativamente, tanto che la stessa nozione di privacy ne risulta significativamente modificata.

Non più privacy intesa come tutela sulla singola conversazione, ma privacy come tutela di tutta la gamma di diverse comunicazioni che riguardano il singolo e si esplicano nell'approvvigionamento di informazioni sulle sue abitudini di vista.

Non si tratta più, dunque, del divieto di carpire una singola e-mail che proviene da un computer, ma del divieto di intercettare e utilizzare tutta una serie di comunicazioni, spesso occulte, che si instaurano tra diversi computer, ogni volta che l'utente preme un tasto viaggiando sulla Rete. Una potenzialità lesiva, invero, che non ha limiti né di spazio né di tempo, e che permette di acquisire le informazioni per poi di rielaborale in modi assolutamente inimmaginabili.

In questo senso, appare forse inadeguato il semplice restyling di un sistema di tutela preesistente e non preparato a queste nuove modalità lesive. Un vecchio problema, quello della tutela della riservatezza delle comunicazioni, che presenta nuovi profili di tutela ai quali far fronte.

In particolare, nel codice penale il legislatore è intervenuto con la l. 547/93 sul titolo XII, del c.p., sez. V, "delitti contro l'inviolabilità dei segreti", prima di tutto estendendo la nozione di "corrispondenza" oltre che a quella epistolare, telegrafica o telefonica, anche a quella "informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza" (art. 616, c. IV) e di "documento" anche a "qualunque supporto informatico contenente dati, informazioni o programmi" (art. 621 c. 2) e di "comunicazioni o conversazioni", e poi inserendo tre nuove fattispecie di reato, l'art. 617 - quater Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; l'art. 617 - quinquies, Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche; l'art. 617 - sexies, Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche. È stato infine inserita a conclusione della sezione, una disposizione che lascia aperto l'ingresso nell'area di inviolabilità del segreto, alla tutela di nuove forme di comunicazioni che nel futuro dovessero prospettarsi: si tratta dell'art. 623 - bis, a norma del quale "le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni, immagini od altri dati".

Nell'insieme, si tratta, tuttavia, di una semplice estensione delle vecchie fattispecie, che si esprime nell'integrazione dei mezzi di comunicazione, che non sono più solo quello cartaceo, telefonico o telegrafico, ma possono essere anche informatico o telematico, mentre invariate sono rimaste le condotte ed uguali le pene.

La disciplina meriterebbe un intervento più approfondito che tenga conto anche delle comunicazioni involontarie quotidianamente effettuate e delle nuove potenzialità lesive di questa invasione della privacy.

In particolare, l'art. 617-quater cp punisce chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico, o intercorrenti tra più sistemi, o le impedisce o le interrompe, o ne rivela il contenuto. L'interesse tutelato dalla norma è chiaramente la riservatezza delle comunicazioni e la libertà e regolarità delle stesse che devono essere libere, complete e senza interruzioni. Com' è ovvio la particolarità del mezzo informatico non incide sul fine delle comunicazioni telematiche, che è comunque la trasmissione di dati tra soggetti in forma riservata.

In proposito, sembra opportuno segnalare che tale previsione è, per così dire, l'alter ego informatico di quanto già previsto per le comunicazioni e conversazioni telefoniche o telegrafiche (art. 617), stante il fatto che il concetto di "intercettazione", assunto nell'art. 617 - quater, corrisponde a "presa di cognizione della comunicazione" di cui all'art. 617.

Sulla stessa lunghezza d'onda si collocano i successivi artt. 617 - quinquies e sexies: altro non sono che l'estensione informatica di quanto già represso dagli artt. 617 - bis e ter.

Si tratta, invero, di previsioni che non sembrano cogliere nel segno della nuova "emergenza" informatica, stante anche il fatto che ad ormai quasi quindici anni dall'ingresso delle suddette norme nel nostro codice le pronunce sono pochissime, tanto si possono contare sulle dita di una mano, mentre altrettanto non sembra potersi dire per la diffusione della violazione della privacy.

GIOVANNI PASCUZZI

Internet e ansia di sicurezza: il rischio informatico

Giovanni Pascuzzi è Professore Ordinario di Diritto Privato Comparato presso la Facoltà di Giurisprudenza dell'Università di Trento dove insegna Diritto Civile. Ha pubblicato numerosi libri e saggi sui rapporti tra diritto e informatica tra cui: Il diritto dell'era digitale: tecnologie informatiche e regole privatistiche, Bologna, Il Mulino, 2006; Cyberdiritto 2.0. Guida alle banche dati italiane e straniere, alla rete Internet e all'apprendimento assistito da calcolatore, (libro e CD interattivo), Bologna, Zanichelli, 2003; Diritto e tecnologie evolute del commercio elettronico, Padova, Cedam, 2004; Diritto e informatica: l'avvocato di fronte alle tecnologie digitali, Milano, Giuffré, 2002; I diritti sulle opere digitali: copyright statunitense e diritto d'autore italiano, Padova, Cedam, 2002 (cur. con Caso R.); Cercare il diritto: libro e CD interattivo, Bologna: Zanichelli, 2005; The law between books and bits, in Droit européen comparé d'internet a cura di Chatillon G., Bruxelles, Bruylant, 2000; Il diritto fra tomi e bit: generi letterari e ipertesti, Padova, Cedam, 1997.

UNA CARATTERISTICA DELL'ERA DIGITALE: L'ANSIA DI SICUREZZA

Il diritto dell'era digitale sembra caratterizzato dall'ansia di sicurezza [1].

Senza sistemi informatici sicuri, il diritto alla protezione dei dati personali si svuoterebbe di significato. Sicura si vuole sia la navigazione in rete, specie per scongiurare il pericolo che i minori abbiano accesso a contenuti nocivi o indecenti. Sicuri devono essere i meccanismi di firma, perché alla loro affidabilità è ancorata la certezza dei traffici. Sicure non possono che essere le transazioni sulla rete (si veda il tema dei protocolli per i pagamenti via rete), se il commercio elettronico deve definitivamente decollare.

SICUREZZA E PROTEZIONE DEI DATI PERSONALI

Nel considerando n. 46 della Direttiva 95/46/CE (tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) si legge: "la tutela dei diritti e delle libertà delle persone interessate relativamente al trattamento di dati personali richiede l'adozione di adeguate misure tecniche ed organizzative sia al momento della progettazione che a quello dell'esecuzione del trattamento, in particolare per garantirne la sicurezza ed impedire in tal modo qualsiasi trattamento non autorizzato; … spetta agli Stati membri accertarsi che il

responsabile del trattamento osservi tali misure; … queste devono assicurare un adeguato livello di sicurezza, tenuto conto delle conoscenze tecniche e dei costi dell'esecuzione rispetto ai rischi che i trattamenti presentano e alla natura dei dati da proteggere".

Muovendo da quanto prescritto nella sezione VIII della direttiva 95/46/CE, il codice della privacy (d. lgs. 30 giugno 2003 n. 196) impone veri e propri obblighi di sicurezza in capo al titolare del trattamento. In particolare l'art. 31 prevede che i dati personali debbano essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L' Allegato B al codice della privacy contiene il disciplinare tecnico in materia di misure minime di sicurezza.

È bene sottolineare che la violazione dell'obbligo di adottare le misure minime di sicurezza (delineate nell'articolo 33 del codice della privacy) è sanzionato penalmente (cfr. art. 169 D. Lgs. 196/2003).

Sul piano civilistico, il trattamento dei dati personali è considerato esercizio di attività pericolosa. Infatti, a norma dell'art. 15 del codice appena citato, chiunque cagioni danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11 che elenca i principi in tema di modalità del trattamento dei dati e requisiti dei medesimi.

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

a. possibile utilizzazione maliziosa e dannosa dei dati personali che riguardano gli individui (e i soggetti diversi dalle persone fisiche);
b. dipendenza sempre maggiore delle società avanzate dai sistemi informatici e telematici: nel considerando n. 1 del Regolamento (CE) n. 460/2004 si legge: "Le reti di comunicazione e i sistemi di informazione sono ormai fattori determinanti dello sviluppo economico e sociale.

Computer e reti stanno diventando strumenti altrettanto comuni dell'acqua corrente o dell'energia elettrica. La sicurezza delle reti di comunicazione e dei sistemi di informazione, in particolare la loro disponibilità, diventa di conseguenza sempre più importante per la società anche a causa della possibilità che si presentino problemi nei sistemi chiave d'informazione a motivo della complessità del sistema, di incidenti, errori e attacchi che possono avere conseguenze sulle infrastrutture fisiche che forniscono servizi essenziali per il benessere dei cittadini dell'UE" [2];

c. vulnerabilità dei sistemi: si veda il considerando n.2 del Regolamento appena citato su cui si tornerà più avanti quando si parlerà di sicurezza e commercio elettronico.

SICUREZZA E DOCUMENTAZIONE

Le nuove tecnologie possono essere utilizzate dall'ordinamento per perseguire finalità tradizionalmente perseguite con altre tecnologie (es.: certezza delle relazioni giuridiche). Si pensi al documento elettronico e alla firma digitale, che grazie a regole all'uopo introdotte (cfr., per il nostro Paese, l'iter che ha portato alla emanazione del Decreto Legislativo 7 marzo 2005, n. 82, "Codice dell'amministrazione digitale" [3]), perseguono le finalità un tempo assicurate da documento cartaceo e sottoscrizione autografa.

Ebbene, anche per il documento informatico rileva il profilo della sicurezza. A norma, ad esempio, dell'art. 21 del Codice dell'amministrazione digitale: "Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza".

SICUREZZA E SOTTOSCRIZIONE

Anche per la firma elettronica si attinge al parametro della sicurezza, specie quando si vuole che la stessa riceva pieno riconoscimento da parte dell'ordinamento in vista del prodursi in capo al titolare degli effetti di volta in volta voluti. La firma elettronica qualificata (di cui la firma digitale è un esempio) deve essere realizzata mediante un dispositivo sicuro (cfr. art. 1, comma 1, lett r del Codice dell'Amministrazione Digitale). In particolare, a norma dell'art. 35 del citato d. lgs. 82/2005, "I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata: a) sia riservata; b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni; c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi".

SICUREZZA E COMMERCIO ELETTRONICO

Nel considerando n. 2 del Regolamento (CE) n. 460/2004 si legge: "Il numero crescente di violazioni della sicurezza ha già provocato notevoli danni economici, turbato la fiducia degli utenti e danneggiato lo sviluppo del commercio elettronico. Gli individui, le amministrazioni pubbliche e le imprese hanno reagito dotandosi di tecnologie e procedure di gestione relative alla sicurezza. Gli Stati membri hanno preso a loro volta numerose misure di sostegno per accrescere la sicurezza delle reti e dell'informazione nella società, come ad esempio campagne di informazione e progetti di ricerca" [4].

Nella seconda metà degli anni '90, con l'esplosione del World Wide Web, la rete diventa strumento per vendere beni e servizi vecchi e nuovi (commercio elettronico). Ci si rende conto che il decollo di siffatte attività sulla rete può essere seriamente ostacolato se i potenziali clienti dovessero sentirsi minacciati da imprecisati rischi. Proprio per accrescere la fiducia dei consumatori nel commercio elettronico, l'Unione Europea ha varato il progetto e-confidence [5].

La sicurezza nel commercio elettronico significa poter essere certi dell'identità dei soggetti che prestano servizi sulla rete (cfr. art. 7 del d. lgs. 70/2003 [6]); ovvero che tali soggetti trattino in maniera leale i dati personali in cui si imbattono nell'espletamento della propria attività [7]; e così via.

SICUREZZA E PAGAMENTI TELEMATICI

Inutile dire che la sicurezza del commercio elettronico riposa anche sulla sicurezza dei pagamenti che avvengono sulla rete. L'utilizzo di mezzi di pagamento via Internet come contropartita della vendita di beni e fornitura di servizi on line presuppone l'esistenza di una infrastruttura tecnologica avanzata e, soprattutto, sicura. Si pensi, a tale proposito, ai protocolli SET (Secure Electronic Transaction) e SSL (Secure Socket Layer). È necessario, inoltre, scongiurare i rischi di frodi, gioco d'azzardo, pratiche di riciclaggio. In argomento si veda la Decisione quadro del Consiglio dell'Unione Europea (2001/413/GAI) del 28 maggio 2001 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti [8], nonché la Direttiva 2005/60/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo [9].

IL RISCHIO INFORMATICO

Il tema della sicurezza informatica è molto sentito [10]. A livello europeo è stata istituita l'Agenzia europea per la sicurezza delle reti e dell'informazione (Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004). L'Agenzia ha il compito di contribuire ad assicurare un elevato livello di sicurezza delle reti e dell'informazione nella Comunità e a sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico nell'Unione europea, contribuendo in tal modo al buon funzionamento del mercato interno.

L'art. 4, comma 1, lett. c) del Regolamento (CE) n. 460/20 definisce "sicurezza delle reti e dell'informazione": la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei relativi servizi forniti o accessibili tramite tale rete o sistema.

Nel considerando n. 19 del Regolamento si legge: "I problemi di sicurezza delle reti e dell'informazione sono questioni globali. Occorre una maggiore cooperazione a livello mondiale per migliorare le norme di sicurezza, migliorare l'informazione e promuovere un approccio globale comune alle questioni legate alla sicurezza delle reti e dell'informazione, contribuendo in tal modo allo sviluppo di una cultura in materia di sicurezza delle reti e dell'informazione. Una cooperazione efficace con i paesi terzi e con la comunità mondiale è ormai un dovere anche a livello europeo. A tal fine l'Agenzia dovrebbe contribuire agli sforzi comunitari in materia di cooperazione con i paesi terzi e, se del caso, con organizzazioni internazionali".

In argomento si vedano anche: la Risoluzione del Consiglio del 18 febbraio 2003 su un approccio europeo per una cultura della sicurezza delle reti e dell'informazione [11]; le Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione. Verso una cultura della sicurezza (luglio 2002) [12]; 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 2002/20/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica (direttiva autorizzazioni).

La sicurezza informatica può essere messa in pericolo da eventi quali:

1. Interruzione o mancanza di servizio (dovuti ad esempio: a catastrofi naturali quali inondazioni o terremoti; incendi; danni fisici alle strutture);
2. Fallimento tecnico del sistema (dovuto, ad esempio, a malfunzionamento dell'hardware, alla mancata entrata in funzione dei sistemi di back up, ovvero ad errori di programmazione);
3. Distruzione, manipolazione o perdita di programmi e dati per eventi diversi da criminalità informatica;
4. Sabotaggio e accesso non autorizzato da parte di dipendenti infedeli;
5. Criminalità informatica tesa all'accesso non autorizzato ovvero alla introduzione di virus, worms, back doors, etc.;

Gli eventi appena ricordati possono produrre una varietà di tipologia di danno:

1. Manipolazione dei siti web;
2. Corruzione e perdita di dati;
3. Violazione di database con connessa violazione di dati personali;
4. Furto di identità;
5. Frodi finanziarie ed economiche (come avviene quando ci si impossessa illecitamente dei numeri di carte di credito);
6. Violazione di segreti industriali;
7. Perdita di profitti;
8. Investimenti per ricostruire l'immagine delle aziende i cui sistemi di sicurezza informatica sono stati violati;
9. Investimenti per ripristinare le apparecchiature e il software.

IL PRINCIPIO DI PRECAUZIONE NELL'ERA DIGITALE ... LA PREVENZIONE DEL RISCHIO INFORMATICO AFFIDATA A TECNOLOGIE EVOLUTE: IL TRUSTED COMPUTING

Il rischio informatico può essere affrontato in modi diversi.

Sul piano legislativo: nelle pagine che precedono sono state ricordate le numerose disposizioni che si occupano di sicurezza informatica.

Sul piano contrattuale: sono sempre più diffuse, ad esempio, le polizze assicurative tese a coprire il patrimonio informatico e le relative responsabilità.

Esiste anche un approccio diverso: è la stessa tecnologia che può apprestare gli strumenti più idonei a garantire la sicurezza informatica.

Conviene approfondire quest'ultima alternativa.

L'approccio tradizionale al rischio informatico si sostanzia nella produzione di strumenti software (antivirus, antispyware e firewall) di reazione ad attacchi ai sistemi informatici ed utilizzi impropri dei computer e delle reti Di recente si sta affermando un approccio del tutto innovativo alla prevenzione del rischio informatico: il Trusted computing [13].

"Trusted Computing" (TC) è una delle molteplici espressioni usate per denominare il coordinamento di alcune iniziative che fanno capo ad imprese leader del settore dell'hardware e del software. Il Trusted Computing Group (TCG) è un'organizzazione no-profit promossa da grandi imprese del settore dell'informatica [14]. Nella presentazione sul sito web di riferimento si legge che gli obiettivi del gruppo sono lo sviluppo e la diffusione di specifiche per standard aperti finalizzati alla produzione di sistemi con architettura "Trusted Computing" composta da elementi hardware e software in grado di essere incorporati su differenti piattaforme, periferiche e dispositivi quali personal computer, palmari e telefoni digitali. Una tale architettura informatica risponderebbe principalmente all'esigenza di rendere più sicuri - ovvero protetti tanto da attacchi compiuti medianti software quanto da attacchi compiuti direttamente sul sistema hardware - la conservazione dei dati, le prassi del business on-line, ed i contratti del commercio elettronico, garantendo la funzionalità del sistema, la privacy ed i diritti individuali.

Il TC si basa su un uso massiccio della crittografia.

L'attuale concezione del TC risponde, infatti, all'obiettivo di creare un ambiente informatico fatto di hardware e software "sicuro", cioè con caratteristiche diverse da quelle di tutti gli altri sistemi informatici. Non è un caso che il TC sia destinato ad essere innervato nelle componenti hardware (un microchip della scheda madre) e software (il sistema operativo) basilari [15], in quanto è proprio l'integrazione tra protezioni hardware e software che - come già accennato - garantisce i massimi livelli di protezione tecnologica attualmente possibili. L'aspetto più significativo della logica del TC sta proprio nella necessità che l'hardware, il software ed i dati dell'utente siano certificati attraverso chiavi crittografiche. Si pone, dunque, il problema della dislocazione del

controllo del sistema informativo dall'utente al certificatore [16] (a ben vedere si passa dal controllo sull'informazione digitale al controllo sulle infrastrutture).

Il TC si presenta dunque come un approccio assolutamente innovativo alla sicurezza informatica. L'obiettivo non è quello di produrre nuovi strumenti software (come antivirus, antispyware e firewall) di reazione ad attacchi ai sistemi informatici ed utilizzi impropri dei computer o delle reti, ma al contrario di promuovere la costruzione di sistemi hardware e software non abilitati a determinate funzioni potenzialmente in grado di comprometterne la sicurezza, nonché il controllo - attraverso Internet - del rispetto delle limitazioni di funzionalità da parte degli utenti dei sistemi.

La logica sottesa al TC è quella del "prevenire è meglio che punire". Un sistema è sicuro o affidabile se il suo hardware ed il suo software sono concepiti e costruiti in modo da essere costretti a funzionare nel modo voluto dai produttori e non dagli utenti finali.

Ciò comporta almeno due conseguenze: da un lato, la limitazione preventiva delle funzionalità del sistema informatico; dall'altro la dislocazione del controllo del sistema informatico dall'utente finale a chi produce l'hardware ed il software, nonché a chi è deputato a sorvegliare che siano rispettate le limitazioni di funzionalità imposte dal produttore. Inutile dire che chiunque controlli l'infrastruttura TC acquisterà un potere considerevole. E non è difficile immaginare i tanti modi nei quali sarebbe possibile abusare di tale potere.

Inoltre, l'approccio TC alla sicurezza informatica pone due problemi di fondo che sono assai rilevanti sul piano giuridico:

a. il processo di elaborazione degli standard tecnologici dell'architettura TC così come la gestione della sicurezza sui cui si basa il TC è nelle mani di privati i quali non necessariamente procedono in base a processi trasparenti o democratici;
b. la sicurezza dipende dall'architettura informatica la quale incorpora non diversamente dalle architetture fisiche alcune regole implicite le quali sono rigide, predeterminate e potenzialmente infallibili [17].

ALCUNI POSSIBILI SCENARI

Il Trusted Computing risponde ad una delle possibili visioni della sicurezza informatica cioè alla logica della "Prevenzione del rischio informatico". Ad un prezzo: quello della "limitazione preventiva delle funzionalità" e della "dislocazione del controllo del sistema informatico dall'utente

ad altri soggetti". Il Trusted Computing sta emergendo come architettura della sicurezza per la prossima generazione di PC. Non è ancora lo standard dominante, ma lo diventerà - con tutta probabilità - nel prossimo futuro. La minaccia alla privacy sta nelle scelte di fondo: limitazione preventiva delle funzionalità e dislocazione del controllo del sistema informatico.

Nel caso del TC la decisione - pur giustificabile in base a molte argomentazioni - dello Stato (o degli Stati) di non ingerirsi direttamente nel processo di standardizzazione delle tecnologie di sicurezza può avere effetti collaterali negativi.

L'adesione all'architettura TC - e dunque ai valori che essa incorpora - potrebbe diventare nel prossimo futuro un prerequisito per l'accesso alla società dell'informazione. Le assicurazioni sul rischio informatico potrebbero essere portate a rafforzare lo standard di fatto. Potrebbero ad esempio rifiutarsi di assicurare le (o potrebbero pretendere polizze esose dalle) imprese che decidono di rifiutare di implementare gli standard TC nei propri sistemi informativi.

Un'ultima notazione. Nella discussione classica sul principio di precauzione in ambito non digitale si discute di come gestire il gap di informazioni ex ante rispetto all'evoluzione tecnologica ed al rischio che essa produce (di qui la difficoltà di definire ed applicare il principio della precauzione e di misurare quanto e quale diritto statale deve regolamentare lo stesso principio). Nel diritto dell'era digitale, dove forse si può disporre di tecnologie che prevengono perfettamente buona parte dei rischi, lasciare la precauzione solo ai privati - intesi come centri di potere normativo privato - implica la certezza che alcuni margini di libertà siano sacrificati. Sotto tale profilo l'incertezza, l'elasticità e la fallibilità del diritto possono avere una valenza positiva [18]. L'ansia, anche quella di sicurezza, in genere non è una buona cosa se supera la soglia di accettabilità. Il rischio fa parte della vita ed è ineluttabile anche quando nascono nuove tecnologie che lo moltiplicano o che lo riducono.

NOTE

[1] Più in dettaglio per i temi trattati nel presente paragrafo, v.: PASCUZZI, Il diritto dell’era digitale, Bologna, 2006, passim.

[2] Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.

[3] PASCUZZI, Il diritto dell’era digitale, cit., 75 ss.

[4] Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.

[5] Sul punto v.: COMMISSIONE DELL'UNIONE EUROPEA, Consumer confidence in E-Commerce: lessons learned from the E-Confidence initiative Brussels, 8 novembre 2004, SEC(2004) 1390, http://europa.eu.int/comm/consumers/cons_int/ecommerce/ e-conf_working_doc.pdf.

[6] Si tratta del Decreto che ha dato attuazione nel nostro Paese alla 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»).

[7] Un ruolo importante nella traiettoria tesa ad avere siti web sicuri può essere giocato da soggetti terzi che si assumono il compito di garantire che i siti si adeguino a precisi standard concedendo ad essi un marchio di qualità. La direttiva 2000/31 sul commercio elettronico invita le associazioni commerciali, professionali e dei consumatori a contribuire all'elaborazione di un quadro affidabile e flessibile per il commercio elettronico definendo codici di condotta. Molto spesso tali codici sono associati ai cosiddetti trustmark schemes (marchi di fiducia) o labels (marchi di qualità garantita). Per quel che riguarda l'Italia, esempio di questo approccio è il certificato Qweb, servizio fornito da IQNET per il tramite di numerosi enti certificatori tra cui RINA e ICQ. Scopo del marchio di qualità è accrescere la fiducia degli acquirenti nei confronti del commercio elettronico, attestando che il fornitore on-line certificato si attiene a determinati principi e criteri nel condurre operazioni commerciali. Il citato marchio Qweb attesta che: il sito è sicuro e registrato legalmente; il servizio di e-business è della migliore qualità; le condizioni di vendita e di consegna sono chiare e veritiere; la sicurezza e la privacy sono applicate per il trattamento dei dati personali; i reclami del cliente sono presi in considerazione e opportunamente gestiti; i consumatori possono ricorrere a una soluzione extragiudiziale delle controversie.

[8] In Gazzetta ufficiale dell'Unione Europea n. L 149 del 2 giugno 2001. V. anche la prima (SEC(2004) 532 - COM/2004/0346 def.) e la seconda (SEC(2006) 188 - COM/2006/0065 def.) Relazione della Commissione fondate sull'articolo 14 della decisione quadro 28 maggio 2001.

[9] In Gazzetta ufficiale dell'Unione Europea n. L 309 del 25 novembre 2005.

[10] A riprova della accresciuta sensibilità al tema, si può segnalare il fatto che nel nostro ordinamento universitario sta per essere introdotta una laurea magistrale in "Sicurezza informatica". Nello schema di decreto relativo alle classi magistrale (elaborato ai sensi del D.M. 270/2004 e relativi allegati, trasmessi al CUN con nota prot.n.Gab/7859.8.1 del 12.9.2006, alla CRUI con nota prot.n. GAB/7860.8.1 e al CNSU con nota prot.n. GAB/7861.8.1 del 12.9.2006) è prevista infatti la classe della laurea magistrale LM 66, intitolata, appunto, Laurea magistrale in Sicurezza informatica. I laureati magistrali nei corsi di laurea della classe devono:

conoscere gli aspetti scientifici relativi alle fondamenta della progettazione, realizzazione, verifica e manutenzione di infrastrutture e sistemi informatici sicuri e protetti;
conoscere le metodologie e gli strumenti tecnologici attraverso i quali si progettano, realizzano, verificano e mantengono infrastrutture e sistemi informatici sicuri e protetti, con attenzione sia alle tecniche formali che sperimentali;
conoscere gli aspetti relativi alla organizzazione del lavoro ed alle problematiche di carattere psicologico e sociale come elementi critici rispetto alla sicurezza delle infrastrutture e dei sistemi informatici ed alla protezione dei dati informatici, nonché gli aspetti giuridici relativi al trattamento sicuro e riservato dei dati informatici e quelli bio-sanitari e bio-etici relativi alle tecniche biometriche ed al trattamento, conservazione e trasmissione dei dati sensibili riguardanti la salute.
[11] 11 GU C 48 del 28 febbraio 2003.

[12] Rinvenibile al sito http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf? OpenDatabase

[13] Diffusamente sull'argomento v.: CASO, Un "rapporto di minoranza": elogio dell'insicurezza informatica e della fallibilità del diritto. Note a margine del trusted computing, in CASO (a cura di), Sicurezza informatica. Regole e prassi, Trento, 2006, 5 ss.

[14] V. il sito web: https://www.trustedcomputinggroup.org.

[15] Per una spiegazione della logica alla base dell'architettura del trusted computing v., in senso critico, ANDERSON, 'Trusted Computing' Frequently Asked Questions, versione 1.1. 2003 (agosto), disponibile all'URL: http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html. Il problema si pone anche per i sistemi di DRM, Digital Rights Management. In argomento v., nella letteratura

italiana, CASO, Digital rights management – Il commercio delle informazioni digitali tra contratto e diritto d'autore, Padova, 2004 (ristampa digitale, Trento, 2006, scaricabile dal sito http://www.jus.unitn.it/users/caso/pubblicazioni/drm/hom e.asp?cod=roberto.caso)

[16] V. le critiche di ANDERSON, 'Trusted Computing' FAQ, cit.

[17] Cfr. CASO, Un "rapporto di minoranza": elogio dell'insicurezza informatica e della fallibilità del diritto. Note a margine del trusted computing, cit.

[18] Cfr., ancora, CASO, Un "rapporto di minoranza": elogio dell'insicurezza informatica e della fallibilità del diritto. Note a margine del trusted computing, cit.

FRANCESCO PIZZETTI

Sicurezza e privacy nelle comunicazioni elettroniche

Francesco Pizzetti, professore Ordinario di diritto costituzionale presso la facoltà di Giurisprudenza dell'Università di Torino. Autore di un centinaio di saggi e articoli scientifici in materia di diritto costituzionale, italiano e comparato, con particolare attenzione ai temi delle riforme istituzionali, dei governi regionali e locali e dei processi di riforma dell'Unione europea. Pro-Rettore dell'Università di Torino (1984-1987), consigliere costituzionale del Presidente del Consiglio Giovanni Goria (1987), vice-Sindaco di Torino (1990-1993), consigliere costituzionale del Presidente del Consiglio Romano Prodi (1996-1998), segretario della Conferenza Stato-città e autonomie locali (1996-1998), consigliere giuridico del Ministro della Funzione Pubblica Franco Bassanini (1996-2001), direttore della Scuola Superiore della Pubblica amministrazione (1998-2001), membro del Consiglio di Presidenza della Giustizia Amministrativa (2000-2004), presidente della Commissione consultiva per le intese con le confessioni religiose, istituita presso la Presidenza del Consiglio dei Ministri (dal 1998), Presidente del Garante per la protezione dei dati personali (dal 2005).

SICUREZZA E PRIVACY: UN BINOMIO POSSIBILE

Sicurezza e Privacy possono costituire due aspetti apparentemente antitetici con cui le società occidentali sono costrette a rapportarsi quotidianamente al fine di stabilire volta per volta quale dei due debba ricevere una minore o maggiore tutela.

La disciplina sulla protezione dei dati personali, in proposito, rappresenta un efficace strumento normativo per attuare un bilanciamento costituzionale tra le due esigenze, regolando attraverso l'enucleazione di taluni principi questo potenziale contrasto. In realtà, a fronte della più recente giurisprudenza del Garante, deve evidenziarsi che la sicurezza, abbinata all'uso delle tecnologie, che rappresentano il più moderno terreno su cui saggiare il livello di tutela della riservatezza, ben si raccorda con la tematica della protezione dei dati, purché ciò avvenga nel rispetto delle regole fissate dall'Autorità di garanzia.

Un'idonea tutela dei diritti dei singoli non pregiudica l'adozione di misure efficaci per garantire la sicurezza dei cittadini e l'accertamento degli illeciti. In generale la rilevazione dei dati a fini di sicurezza (in senso lato) è possibile solo se fondata su uno dei presupposti di liceità che il Codice in

materia di protezione dei dati personali [1] (di seguito "Codice") prevede espressamente, e in modo differenziato, per i soggetti pubblici da un lato e per i soggetti privati e gli enti pubblici economici dall'altro. Gli scopi perseguiti dalla raccolta di informazioni devono essere determinati, espliciti e legittimi. Possono essere perseguite solo finalità di pertinenza del titolare del trattamento, finalità determinate e rese conoscibili.

Nel valutare la necessità di utilizzare uno strumento di rilevazione in relazione al grado di rischio presente in concreto, deve evidenziarsi che tali sistemi possono essere attivati solo quando altre misure siano state ponderatamente valutate come insufficienti o inattuabili. Se le stesse sono finalizzate alla protezione di beni, devono risultare parimenti inefficaci altri accorgimenti quali controlli da parte di addetti, sistemi di alert, misure di protezione degli accessi, abilitazioni agli accessi. Non va, pertanto, adottata la scelta semplicemente meno costosa, o meno complicata, o di più rapida attuazione, che potrebbe non tener conto dell'impatto sui diritti degli altri cittadini o di chi abbia diversi legittimi interessi.

Poiché l'adozione di sistemi automatizzati di rilevazione comporta l'introduzione di un vincolo per il cittadino, il sistema informativo e il relativo programma informatico vanno conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi. Il software va configurato anche in modo da cancellare periodicamente e automaticamente i dati eventualmente registrati qualora questi non risultassero più funzionali al perseguimento delle lecite finalità del trattamento.

Il binomio Privacy e sicurezza acquista una valenza ulteriore se si considera che l'integrità dei dati relativi all'utente è garantita dall'adozione delle misure minime previste dal Codice. Se, infatti, l'implementazione di sistemi di sicurezza, ove implichi una rilevazione di informazioni dell'interessato, rappresenta un trattamento di dati personali, peraltro non soggetto al consenso di quest'ultimo in quanto misura necessaria per adempiere ad obblighi di legge ai sensi dell'art. 24 del Codice, è pur vero che l'assenza di misure di sicurezza idonee a garantire i diritti dell'interessato è causa di illiceità del trattamento e di inutilizzabilità dei dati medesimi. Negli ultimi anni, il Garante ha dettato ai fornitori di servizi di comunicazione numerose prescrizioni in materia di sicurezza, sia in riferimento all'attività da essi svolta a supporto delle indagini delle autorità giudiziarie, sia per quanto concerne l'ordinaria conservazione sicura dei dati relativi alle comunicazioni degli interessati.

MISURE DI SICUREZZA NELL'AMBITO DELLE INTERCETTAZIONI

Il tema del trattamento dei dati connessi alle intercettazioni effettuato da fornitori di servizi telefonici riveste particolare importanza, sia in riferimento alla garanzia della sfera personale degli indagati (e delle altre persone estranee alle indagini, ma coinvolte nelle comunicazioni e conversazioni), sia per quanto concerne la tutela dell'interesse pubblico alla segretezza delle indagini.

Pur non dovendo venire a conoscenza dei "contenuti", i fornitori raccolgono, selezionano ed elaborano una notevole quantità di dati personali riferibili agli indagati e ai terzi con i quali questi ultimi comunicano. Si tratta di dati personali riservati e delicati che attengono, in particolare, all'identità dei soggetti sottoposti a intercettazione, all'arco temporale di svolgimento dell'intercettazione e ai dati di traffico telefonico o telematico inerenti alle linee intercettate (data, ora, numero chiamato e durata della comunicazione o conversazione).

A seconda dei casi, tenendo conto delle specifiche richieste dell'autorità giudiziaria, i medesimi dati sono integrati da informazioni tecniche aggiuntive relative ai dettagli delle chiamate entranti, ai tentativi di chiamata in entrata o in uscita e ai dati di localizzazione geografica dell'utenza intercettata. Le intercettazioni telematiche sono quantitativamente meno rilevanti rispetto a quelle telefoniche e riguardano in prevalenza sia il traffico Ip sviluppato su linee telefoniche o collegamenti a larga banda, sia comunicazioni tramite posta elettronica. Queste ultime vengono realizzate predisponendo un inoltro automatico della corrispondenza ricevuta e spedita dall'intercettato verso un'utenza di posta elettronica messa a disposizione dal fornitore.

Nel 2006 il Garante ha prescritto ai principali fornitori la necessità di garantire che gli organi aziendali cui compete lo svolgimento di servizi per conto dell'autorità giudiziaria adottino un modello organizzativo in grado di limitare al minimo la conoscibilità delle informazioni relative alle attività svolte per esigenze di giustizia, con una rigida partizione della visibilità dei dati su base organizzativa, funzionale e di area geografica di competenza. Il personale che a qualsiasi titolo tratti questi dati deve essere designato in termini selettivi quale incaricato del trattamento; particolare rigore deve essere assicurato nella gestione e nel mantenimento della qualità delle credenziali di autenticazione per l'accesso informatico ai dati trattati, conformando le procedure di gestione delle credenziali e i sistemi di autorizzazione a principi rigidi di coerenza delle abilitazioni nei sistemi informativi con i ruoli e le funzioni assegnate agli incaricati designati.

Deve essere altresì realizzata, anche attraverso un'opportuna configurazione dei sistemi informatici utilizzati, una separazione marcata tra i dati di carattere amministrativo-contabile e i dati documentali prodotti nel corso delle operazioni svolte su richiesta dell'autorità giudiziaria, inibendo la possibilità per un operatore amministrativo-contabile di accedere ai dati documentali prodotti. I fornitori devono provvedere affinché l'interscambio di informazioni con l'autorità giudiziaria avvenga evitando il ricorso a canali non affidabili, o affidabili solo parzialmente, sia dal punto di vista delle prestazioni, sia da quello della sicurezza, adottando a tal fine sistemi di comunicazione basati su aggiornati strumenti telematici sviluppati con protocolli di rete sicuri.

Il Garante ha poi ritenuto necessario che i fornitori sviluppino o integrino strumenti informatici idonei ad assicurare il controllo delle attività svolte da ciascun incaricato sui singoli elementi di informazione presenti nei data-base utilizzati. Tutti i dati personali acquisiti o formati per scopi di giustizia devono essere protetti con moderni strumenti di cifratura, precludendo la loro conoscibilità da parte di soggetti non legittimati.

LA CONSERVAZIONE DEI DATI DI TRAFFICO E LE INDICAZIONI DELL'UNIONE EUROPEA

Il tema della conservazione dei dati di traffico (telefonico e telematico) è stato oggetto di grande attenzione da parte del Garante che, nel 2006, ha avviato una serie di complessi accertamenti in loco nei confronti di numerosi gestori telefonici.

Il Codice, pur fornendo una definizione generale di "dati relativi al traffico", non distingue i dati relativi al traffico "telefonico" da quelli relativi al traffico "telematico".

L'attuale disciplina in tema di data retention dettata dall'art. 132 prescrive ai fornitori di servizi di comunicazione elettronica di conservare, per finalità di accertamento e repressione dei reati, i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, e i dati relativi al traffico telematico, esclusi i contenuti delle comunicazioni, rispettivamente per ventiquattro e sei mesi, prevedendo un periodo ulteriore di conservazione, rispettivamente di ventiquattro e sei mesi, per l'accertamento e la repressione dei delitti individuati dall'art. 407, comma 2, lett. a), c.p.p., nonché dei delitti in danno di sistemi informatici o telematici (art. 132, comma 2).

La materia della data retention sarà interessata da nuove valutazioni di carattere normativo, anche per effetto del prossimo recepimento della direttiva 2006/24/CE approvata il 15 marzo 2006 [2], che

contiene chiare e precise indicazioni sul risultato atteso a livello comunitario in ordine, tra l'altro, alla corretta e uniforme individuazione delle categorie di dati da conservare, in relazione agli specifici servizi enucleati, quali telefonia di rete fissa e telefonia mobile, accesso Internet, posta elettronica e telefonia via Internet.

La direttiva è stata oggetto di numerosi rilievi nel parere espresso preventivamente dalle Autorità europee per la protezione dei dati personali (parere elaborato da un sottogruppo che è stato coordinato dall'Autorità italiana: parere del Gruppo art. 29, Wp 113, 21 ottobre 2005) [3] e nel parere successivo alla Sua adozione (parere Gruppo art. 29, Wp 119, 25 marzo 2006) [4].

In tale occasione, infatti, le Autorità di protezione dei dati hanno chiesto che, in sede di recepimento, ogni Stato provveda a garantire che le disposizioni emanate dal legislatore comunitario siano interpretate e attuate secondo modalità armonizzate, tali da assicurare ai cittadini il medesimo grado di tutela in tutta l'Unione europea.

A fronte di tali considerazioni il Gruppo art. 29 ha rilevato in particolare la necessità di prevedere: l'indicazione precisa dello scopo della conservazione; la limitazione dell'accesso ai dati (i dati devono essere disponibili soltanto ad autorità pubbliche, specificamente individuate in un elenco reso pubblico, quando tale accesso sia necessario ai fini di indagini rivolte all'accertamento ed al perseguimento dei reati menzionati nella direttiva; di ogni accesso deve essere mantenuta una registrazione (log); occorre inoltre un controllo sulle registrazioni da parte dell'autorità di vigilanza); selezione dei dati da utilizzare per le finalità per le quali è consentita la conservazione (le indagini, gli accertamenti e il perseguimento di reati gravi non devono comportare il recupero generalizzato, da parte delle autorità giudiziarie e di polizia, dei dati riguardanti le abitudini e le comunicazioni di persone non sospette); misure di sicurezza (devono essere definite norme riguardanti le misure di sicurezza di natura tecnica ed organizzativa che i suddetti prestatori di servizi devono adottare).

LA SALVAGUARDIA DELLA RETE NELLA NORMATIVA COMUNITARIA SULLE COMUNICAZIONI ELETTRONICHE

Negli ultimi mesi del 2005 è stata avviata la revisione del "pacchetto normativo comunitario" in materia di comunicazioni elettroniche, che riguarda anche la direttiva 2002/58/CE (la cd. "direttiva e-Privacy")[5]. La Commissione europea dopo aver pubblicato nel giugno 2006 una "comunicazione" sulla revisione del quadro normativo, che affronta anche la questione delle

eventuali modifiche alla direttiva e-Privacy, ha avviato nel mese di luglio 2006 una consultazione pubblica. A tale consultazione il Gruppo dei garanti europei ha contribuito con un documento adottato il 26 settembre 2006 (Wp 126) [6]. Le proposte di modifica avanzate dalla Commissione si limitano sostanzialmente agli aspetti di "sicurezza" delle reti di comunicazione e alla necessità di aumentare i poteri delle autorità nazionali; pertanto, l'impianto complessivo della direttiva 2002/58/CE sembrerebbe destinato a rimanere inalterato. Nel suo parere, il Gruppo ha accolto con favore questa posizione della Commissione, pur sottolineando alcune incongruenze: in via generale, il potenziamento delle misure di sicurezza non può tradursi in provvedimenti tali da comprimere la riservatezza o facilitare la sorveglianza delle comunicazioni elettroniche; rispetto alla proposta di obbligare i fornitori di servizi a segnalare non soltanto i possibili rischi per la sicurezza delle reti di comunicazione, ma anche le violazioni concretamente verificatesi, il Gruppo ha proposto di estendere tale possibilità alla totalità degli utenti e non solo alle potenziali "vittime"; è necessaria maggiore chiarezza rispetto alla questione della responsabilità, ossia se gli obblighi previsti dalla direttiva siano applicabili ai fornitori di infrastrutture per l'accesso, ai fornitori di servizi, o ad entrambi. Su questo punto il Gruppo ha richiamato le osservazioni formulate nel proprio parere (Wp 36) reso nel 2000 in occasione dei lavori preparatori della direttiva 2002/58/CE [7]. Infine, l'incremento dei poteri delle autorità di garanzia non dovrebbe tradursi in un onere eccessivo o improprio; in particolare, secondo il Gruppo, non spetta alle autorità di protezione dei dati fissare i criteri tecnici per l'attuazione delle misure di sicurezza eventualmente indicate, che dovrebbero invece essere sviluppati dai soggetti preposti alla regolazione specifica del settore delle comunicazioni elettroniche.

IL CODICE DEONTOLOGICO DEGLI OPERATORI DELLA RETE

Nel nostro Paese, il rapporto tra utenti della rete e gli operatori internet, anche in relazione alle finalità correlate al perseguimento della "sicurezza" pubblica o privata, sarà disciplinato nel dettaglio dal codice deontologico per gli operatori Internet previsto dall'art. 133 del Codice, che consentirà di introdurre specifiche garanzie quali ulteriori presupposti di liceità e correttezza dei trattamenti di dati personali on-line. Il "codice Internet", attualmente in fase di definizione, intende indicare soluzioni effettive, adeguate e dinamiche a talune questioni al fine di sensibilizzare maggiormente gli utenti sui rischi derivanti dall'utilizzo della rete (offrendo loro ulteriori opportunità di tutela) e di indicare ai diversi operatori interessati concreti strumenti per adempiere agli obblighi di legge, assicurando un più elevato livello di rispetto della normativa sulla protezione dei dati personali.

La sottoscrizione di tale codice è stata promossa dal Garante nell'ambito delle associazioni rappresentative degli operatori del settore. Nell'ambito dei lavori preparatori del codice di deontologia sono state affrontate diverse esigenze concrete ed attuali fra le quali quelle relative: all'obbligo di informare adeguatamente gli utenti circa i possibili trattamenti, impliciti o espliciti, che possono riguardarli; al consenso da manifestare espressamente e liberamente; ai presupposti e ai limiti entro i quali è legittimo l'uso di marcatori o dispositivi analoghi on-line; alle modalità semplificate per esercitare i diritti di cui all'art. 7 del Codice; alle caratteristiche di sicurezza per evitare l'aggravarsi del fenomeno del cd. "furto d'identità", già indicato tra le primissime minacce della sicurezza in rete da numerosi documenti internazionali.

LA SICUREZZA IN RETE COME FATTORE DI ACCRESCIMENTO DELLA FIDUCIA DEGLI UTENTI

La parola italiana "fiducia" corrisponde semanticamente a due distinti termini inglesi, ciascuno implicante una diversa esigenza diffusa nella rete Internet: da un lato "fiducia" corrisponde, infatti, a (web) "trust", cioè all'esigenza di transazioni sicure, dall'altro traduce (web) "confidence", nel senso di protezione della privacy compatibile con le regole di comunicazione della comunità virtuale.

Ottenere la "fiducia" del consumatore nei due sensi indicati è un fattore fondamentale per la trasparenza e l'affidabilità delle attività on-line. Infatti, la mancanza di sicurezza-fiducia che si riconnette alla mancanza di controllo sui propri dati e dispositivi non può che determinare nel medio termine, a cascata, effetti di censura dei siti web, dei contenuti digitali, di fidelizzazione forzata degli utenti ed, in ultima analisi, di crollo degli standard per l'interscambio delle informazioni.

Di recente, indagini "sul campo" sembrerebbero evidenziare una crescita del numero di consumatori on-line disposti a ricevere una personalizzazione più efficace, rendendo disponibili maggiori informazioni personali affinché l'esperienza di acquisto on-line diventi più soddisfacente.

I risultati di tali ricerche, a ben vedere, evidenziano da parte degli utenti, la consapevolezza della necessità che sia garantita la sicurezza delle proprie informazioni. Diviene perciò fondamentale l'esigenza di sicurezza e di affidabilità dei sistemi, abbinata ad una maggiore trasparenza da parte dei fornitori in grado di indicare chiaramente, in tempo reale, cosa sta accadendo in ogni passaggio on-line affinché la personalizzazione sia "amichevole" e non risulti "sospetta", inducendo un

chilling effect. L'accento, quindi, sembra destinato a spostarsi progressivamente, dal momento della raccolta, sulle garanzie di qualità del trattamento, sulla sicurezza e sull'informativa preventiva, seguendo una linea che da tempo i Garanti europei e le organizzazioni internazionali come l'OCSE hanno individuato come nuova frontiera di protezione dei diritti individuali.

Tali temi, poi, sono destinati ad essere affrontati su base internazionale, in sede di cooperazione transfrontaliera o di accordi tra gli Stati, ma anche su base di autoregolazione, ovvero attraverso il riconoscimento di nuovi diritti ai consumatori.

I medesimi tratti di tendenza sono del resto riconoscibili nelle più recenti iniziative internazionali nella materia. Gli Stati Uniti, ad esempio, hanno approvato alla fine del 2006 una nuova legislazione specifica su Internet, il cd. US SAFE WEB Act ("Undertaking Spam, Spyware, And Fraud Enforcement with Enforcers beyond Borders Act of 2006"), per limitare spam, spyware e furti di identità anche attraverso la cooperazione transfrontaliera. Qualche settimana fa, l'OCSE ha adottato una raccomandazione sulla cooperazione tra Stati per scopi di enforcement delle normative sulla privacy rispetto ai flussi transfrontalieri di dati ed al loro trattamento on-line. In Europa, la decisione 854/2005/CE del Parlamento europeo e del Consiglio dell' 11 maggio 2005 [8] ha istituito un nuovo programma comunitario pluriennale finalizzato a promuovere un uso più sicuro di Internet e delle nuove tecnologie on-line (Safer Internet Plus), che incoraggia l'uso di misure di tipo tecnologico per contrastare contenuti indesiderati e nocivi e migliorare il livello di riservatezza in conformità alle direttive [9] 2002/58/CE e 95/46/.

NOTE

[1] Decreto legislativo 30 giugno 2003, n. 196.

[2] Direttiva n. 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell’ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GUCE N. L 105 del 13/04/2006).

[3] Gruppo art. 29, Parere 4/2005 sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell’ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE (COM (2005) 438 definitivo del 21.9.2005), adottato il 21 ottobre 2005 (Wp 113).

[4] Gruppo art. 29, Parere 3/2006 sulla direttiva 2006/24/CE del Parlamento europeo e del Consiglio riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, adottato il 25 marzo 2006 (Wp 119).

[5] Direttiva n. 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GUCE N. L 201 del 31/7/2002).

[6] Gruppo art. 29, Parere 8/2006 sulla revisione del quadro normativo per le reti e i servizi di comunicazione elettronica, con particolare attenzione alla direttiva relativa alla vita privata e alle comunicazioni elettroniche, adottato il 26 settembre 2006 (Wp 126).

[7] Gruppo art. 29, Parere 7/2000 sulla proposta della Commissione europea di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche del 12 luglio 2000 (COM (2000) 385), adottato il 2 settembre 2000 (Wp 36).

[8] Decisione n. 854/2005/CE del Parlamento europeo e del Consiglio dell'11 maggio 2005 che istituisce un programma comunitario pluriennale inteso a promuovere un uso più sicuro di Internet e delle nuove tecnologie on line (GUCE L 149 dell'11.6.05).

[9] Direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GUCE N. L 281/40 del 23/11/1995).

STEFANO RODOTÀ

Parlamenti e sviluppo della società dell'informazione

Stefano Rodotà, (Cosenza, 1933) insegna Diritto civile nell'università di Roma "La Sapienza".
È stato Presidente dell'Autorità garante per la protezione dei dati personali e del Gruppo europeo dei Garanti.
È stato parlamentare italiano ed europeo. Ha scritto molte opere sui rapporti tra tecnologie e diritti.

Qual è il destino dei parlamenti nell'età dell'informazione e della comunicazione? Alcuni anni fa, quando cominciò il dibattito sulla democrazia elettronica, sembrava che le nuove tecnologie avrebbero portato ad una progressiva scomparsa della democrazia rappresentativa, sostituita da forme sempre più diffuse di democrazia diretta. Nel nuovo agorà elettronico i cittadini avrebbero potuto prendere sempre la parola e decidere su tutto.

La memoria dell'antica Atene e il modello dei town meetings del New England apparivano come la forma nuova della democrazia, con un intreccio tra antico e nuovo che avrebbe via via cancellato il ruolo dei parlamenti. Nel 1994, un influente uomo politico americano, Newt Gingrich, che sarebbe diventato Speaker della Camera dei Rappresentanti, parlava di un "Congresso virtuale", che avrebbe sostituito il Congresso tradizionale, affidando al voto elettronico di tutti i cittadini anche le scelte legislative.

Oggi queste ipotesi sono lontane, e la democrazia elettronica segue strade diverse da quelle di una brutale e ingannevole semplificazione dei sistemi politici. Ma questo non vuol dire che i parlamenti possano trascurare le grandi novità determinate dalle tecnologie dell'informazione e della comunicazione, che incidono profondamente sul loro ruolo e sul modo in cui si struttura il loro rapporto con la società. Non siamo di fronte a semplici strumenti tecnici, ma ad una forza potente, la tecnologia nel suo complesso, che sta trasformando in modo radicale le nostre società. Stiamo passando, su scala mondiale, da un equilibrio tecnologico all'altro. E un grande antropologo, Marvin Harris, ha sottolineato che "il momento decisivo per una scelta consapevole si ha soltanto durante la fase di transizione da un modo di produzione all'altro. Dopo che una società ha scelto una particolare strategia tecnologica ed ecologica per risolvere il problema dell'efficienza declinante, può essere impossibile modificare le conseguenze di una scelta poco intelligente per un lungo periodo futuro". Il primo, grande compito dei parlamenti, oggi, è dunque quello di cogliere questo

momento, di compiere tempestivamente le scelte intelligenti necessarie perché l'insieme delle tecnologie si risolva in un rafforzamento complessivo della democrazia.

Sono divenute chiare alcune linee di analisi e di intervento, che possono essere così riassunte:

- evitare che le nuove tecnologie dell'informazione e della comunicazione portino ad una concentrazione invece che ad una diffusione del potere sociale e politico;
- evitare che le nuove tecnologie, invece di favorire una vera partecipazione dei cittadini, si consolidino come la forma del populismo del nostro tempo, con un continuo scivolamento verso la democrazia plebiscitaria;
- evitare che ci si trovi sempre più visibilmente di fronte a tecnologie del controllo invece che a tecnologie delle libertà;
- evitare che nell'età dell'informazione e della comunicazione nuove disuguaglianze si aggiungano a quelle esistenti;
- evitare che il grande potenziale creativo delle nuove tecnologie porti non ad una diffusione della conoscenza come grande bene comune, ma a forme insidiose di privatizzazione.

Pure l'età digitale, dunque, ha i suoi peccati, sette come vuole la tradizione, e che sono stati così enumerati: 1) diseguaglianza; 2) sfruttamento commerciale e abusi informativi; 3) rischi per la privacy; 4) disintegrazione delle comunità; 5) plebisciti istantanei e dissoluzione della democrazia; 6) tirannia di chi controlla gli accessi; 7) perdita del valore del servizio pubblico e della responsabilità sociale. Non mancano, tuttavia, le virtù, prima tra tutte l'opportunità grandissima di dare voce a un numero sempre più largo di soggetti individuali e collettivi, di produrre e condividere la conoscenza, sì che ormai molti ritengono che la definizione che meglio descrive il nostro presente, e un futuro sempre più vicino, sia proprio quella di "società della conoscenza". Al di là delle immagini e delle metafore, i parlamenti non sono chiamati a scegliere tra il bene e il male. Di fronte ad una realtà complessa, nella quale convivono società della conoscenza e società del rischio, i parlamenti devono ribadire la loro storica e insostituibile funzione di custodi della libertà e dell'eguaglianza.

Non sono riferimenti retorici. La tecnologia è prodiga di promesse. Alla democrazia offre strumenti per combattere l'efficienza declinante, e arriva fino a proporne una rigenerazione. Ma, se guardiamo al mondo reale, alle tendenze in atto, rischiamo di incontrare sempre più spesso un uso delle tecnologie che rende capillare e continuo il controllo dei cittadini. A queste tendenze bisogna reagire, non solo per sfuggire ad una sorta di schizofrenia istituzionale che spinge verso la

costruzione di un mondo diviso tra le speranze di libertà e l'insidia della sorveglianza è necessario soprattutto considerare realisticamente le dinamiche sociali, a cominciare da quelle che rischiano di produrre nuove diseguaglianze.

Questo problema viene solitamente indicato con l'espressione digital divide, ed effettivamente l'uso delle tecnologie, di Internet in primo luogo, produce stratificazioni sociali, l'emergere di nuove categorie di haves e di have nots, di abbienti e non abbienti proprio per quanto riguarda la fondamentale risorsa dell'informazione. Ma le più attendibili ricerche sul digital divide mettono in evidenza che il divario tra paesi sviluppati e paesi meno sviluppati, per quanto riguarda l'accesso ad Internet, non può essere esaminato riferendosi prevalentemente alle differenze di reddito. Pur rimanendo profondissime, infatti, le distanze riguardanti Internet tendono a ridursi più rapidamente di quelle relative alla ricchezza. Questo vuol dire che i fattori influenti non sono tanto quelli economici, quanto piuttosto quelli sociali e culturali, sì che l'attenzione deve essere in particolare rivolta alle politiche dell'accesso ad Internet, tuttavia in una prospettiva che non si limiti a favorire l'accesso in sé, ma si preoccupi delle modalità d'uso e dei contenuti ai quali è possibile accedere. Altrimenti, non solo la propensione all'accesso ad Internet rimane più bassa per i paesi e i ceti più svantaggiati, ma le fonti della disuguaglianza persistono e tendono ad ampliarsi.

Questa è una indicazione assai importante per le politiche di sviluppo che i parlamenti devono promuovere, e per la cooperazione internazionale. Quando, infatti, l'accesso non è considerato soltanto nella prospettiva, pur importantissima, di assicurare a tutti la connettività alla rete, esso deve essere pensato in termini di accesso alla conoscenza, con evidente incidenza sulle politiche della formazione, della libertà, della proprietà.

Conoscenza è parola che sintetizza le possibilità di accedere alle fonti, di elaborare il materiale raccolto, di diffondere liberamente le informazioni. Già nell'articolo 19 della Dichiarazione universale dei diritti dell'uomo delle Nazioni Unite si è affermato il diritto di ogni individuo alla libertà di opinione e di espressione "e quello di cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo a frontiere". Oggi questo diritto è in pericolo per la pretesa di molti Stati di controllare Internet, per l'esercizio di veri poteri di censura, per le condanne di autori di quelle particolari comunicazioni in rete che sono i blog. Questa situazione non può essere ignorata, soprattutto perché alcune grandi società - Microsoft, Google, Yahoo!, Vodafone - hanno annunciato per la fine dell'anno la pubblicazione di una "Carta" per tutelare la libertà di espressione su Internet. I parlamenti non possono accettare che la garanzia del free speech, che gli Stati Uniti

vollero affidare al Primo Emendamento della loro Costituzione, divenga materia di cui si occupano solo i privati, che evidentemente offriranno solo le garanzie compatibili con i loro interessi. Sono urgenti in questa materia iniziative dei parlamenti nazionali, tuttavia coordinate tra loro dato il carattere transnazionale dei fenomeni da regolare, e tenendo conto che nell'Internet governance Forum, organizzato dall'Onu alla fine dell'anno scorso, è stata esplicitamente indicata la priorità rappresentata dalla elaborazione di un Internet Bill of Rights.

Internet è il più grande spazio pubblico che l'umanità abbia conosciuto, dove si sta realizzando anche una grande redistribuzione di potere. Un luogo dove tutti possono prendere la parola, acquisire conoscenza, produrre idee e non solo informazioni, esercitare il diritto di critica, dialogare, partecipare alla vita comune, e costruire così un mondo diverso di cui tutti possano egualmente dirsi cittadini. Ma tutto questo può diventare più difficile, per non dire impossibile, se la conoscenza viene chiusa in recinti proprietari senza considerare proprio la novità della situazione che abbiamo di fronte e che impone di guardare alla conoscenza come il più importante tra i beni comuni.

La questione dei beni comuni è essenziale. Parole nuove percorrono il mondo - open source, free software, no copyright - dando il senso di un cambiamento d'epoca. Oggi, infatti, il conflitto tra interessi proprietari e interessi collettivi non si svolge soltanto intorno a risorse scarse, in prospettiva sempre più drammaticamente scarse come l'acqua. Nella dimensione mondiale assistiamo ad una creazione incessante di nuovi beni, la conoscenza prima di tutto, rispetto ai quali la scarsità non è l'effetto di dati naturali, ma di politiche deliberate, di usi impropri del brevetto e del copyright, che stanno determinando un movimento di "chiusura" simile a quello che, in Inghilterra, portò alla recinzione delle terre comuni, prima liberamente accessibili. Questa scarsità artificiale, creata, rischia di privare milioni di persone di straordinarie possibilità di crescita individuale e collettiva, di partecipazione politica.

La sfida lanciata ai parlamenti non riguarda soltanto la necessità di trovare nuovi equilibri tra logica della proprietà e logica dei beni comuni. Investe lo stesso modo d'intendere la cittadinanza. La vera novità democratica delle tecnologie dell'informazione e della comunicazione, infatti, non consiste nel dare ai cittadini l'ingannevole illusione di partecipare alle grandi decisioni attraverso referendum elettronici. Consiste nel potere dato a ciascuno e a tutti di servirsi della straordinaria ricchezza di materiali messa a disposizione dalle tecnologie per elaborare proposte, controllare i modi in cui viene esercitato il potere, organizzarsi nella società. Con questo vasto mondo - in cui la democrazia

si manifesta in maniera "diretta", ma senza sovrapporsi a quella "rappresentativa" - i Parlamenti devono trovare nuove forme di comunicazione, attraverso consultazioni anche informali, messa in rete di proposte sulle quali si sollecita il giudizio dei cittadini, procedure che consentano di far giungere in parlamento proposte elaborate da gruppi ai quali, poi, vengano riconosciute anche possibilità di intervento nel processo legislativo. La rigida contrapposizione tra democrazia rappresentativa e democrazia diretta potrebbe così essere superata, e la stessa democrazia parlamentare riceverebbe nuova legittimazione dal suo presentarsi come interlocutore continuo della società.

In questa prospettiva, i parlamenti debbono rafforzare il loro ruolo in diverse direzioni. Promuovere la trasparenza nell'intero sistema istituzionale, rendendo così più efficace il controllo diffuso da parte dei cittadini, la loro "cittadinanza attiva", che diventa anche uno strumento essenziale per la lotta alla corruzione. Non dimentichiamo quel che disse Louis Brandeis, il grande giudice della Corte suprema degli Stati Uniti: "la luce del sole è il miglior disinfettante". Debbono agire come centro che promuove la conoscenza dei cittadini sulle questioni socialmente rilevanti. Debbono divenire il luogo istituzionale dove si svolge con continuità la valutazione degli effetti delle nuove tecnologie, riprendendo e aggiornando l'esperienza del "technology assessment". Ma debbono soprattutto impedire che le esigenze di lotta a terrorismo e criminalità e le richieste del sistema economico portino alla nascita di una società della sorveglianza, della selezione e del controllo, alterando quel carattere democratico dei sistemi politici di cui proprio i parlamenti sono i primi ed essenziali garanti.

Proprio le tecnologie, con la loro apparente neutralità, hanno rafforzato le spinte verso la creazione di gigantesche raccolte di dati personali. La politica sta delegando alla tecnica la gestione dei più diversi aspetti della società, dimenticando, ad esempio, un principio chiaramente indicato nell'articolo 8 della Convenzione europea dei diritti dell'uomo. In questa norma si ammettono limitazioni dei diritti per diverse finalità, compresa la sicurezza nazionale, a condizione però che si tratti di misure compatibili con le caratteristiche di una società democratica. I parlamenti devono esercitare con il massimo rigore questa funzione di controllo, senza delegarla ad altri organi dello Stato, fossero pure le corti costituzionali. Solo così possono evitare la trasformazione dei cittadini in sospetti, ed impedire che, con l'argomento della difesa della democrazia, sia proprio la democrazia ad essere perduta.

Queste considerazioni possono apparire poco realistiche, soprattutto se si considera la notevole riduzione di poteri che, per diverse ragioni, i parlamenti hanno conosciuto in questi anni. Il potere si è notevolmente spostato nella direzione dei governi, molte possibilità di azione sono ormai escluse dal fatto che la sede delle decisioni si colloca fuori dagli Stati nazionali. Ma proprio la riflessione sulle tecnologie ci indica la possibilità di un cammino diverso.

Sulla scena nazionale ed internazionale compaiono attori sempre più numerosi. Si stenta a trovare un centro del sistema istituzionale, tanto che si è parlato di uno "Stato a rete", sottolineando proprio il fatto che le tecnologie promuovono la crescita di una molteplicità di centri di decisione che riescono ad agire grazie alle forme di collegamento via via apprestate dallo sviluppo delle tecnologie dell'informazione e della comunicazione. Ma l'osservazione della realtà ci dice che queste tecnologie non producono soltanto forme di policentrismo, di distribuzione dei tradizionali poteri sovrani tra soggetti non gerarchizzati. Rendono possibile anche centralizzazione e concentrazione dei poteri, esercizio di controlli di intensità senza precedenti. Questa deriva pericolosa può essere interrotta se i parlamenti riusciranno a sottrarre la politica alla seduzione di una tecnologia che deresponsabilizza, che si presenta come un rifugio dove la politica sfugge alla difficoltà delle scelte, ed utilizzeranno, invece, proprio le tecnologie dell'informazione e della comunicazione per far sì che le scelte possano tornare ad essere patrimonio di soggetti visibili, responsabili, controllabili.

La politica come "rete", peraltro, offre all'antica istituzione parlamentare non una occasione di ringiovanimento, ma la possibilità di collegamenti che consentano ai diversi parlamenti, al di là delle frontiere, la comune consapevolezza dei problemi da affrontare. La cooperazione tra i parlamenti non è più una formula, ma una opportunità concreta che nasce dalla crescente possibilità di conoscenze comuni, di circolazione continua di informazioni. Da qui può nascere una nuova sfera pubblica mondiale, non più consegnata alle sole dinamiche dei mercati, ma riguadagnata alla logica dei poteri democratici.

FULVIO SARZANA DI SANT' IPPOLITO

Il digital divide e le telecomunicazioni: potenziali soluzioni tecnico regolamentari

Fulvio Sarzana di Sant'Ippolito, è titolare dello Studio Legale Sarzana e Associati con sedi a Roma e Milano. Nel Corso della sua attività professionale si è occupato principalmente di vicende legate alla regolamentazione dell'informatica e delle telecomunicazioni e ha partecipato, in qualità di consigliere giuridico di Associazioni di operatori di comunicazione elettronica, a diversi tavoli di lavoro Ministeriali per la regolamentazione dell'ICT. È stato Professore a contratto di "Regolazione dei sistemi mediali", di "Gestione dei diritti e delle opere multimediali" e di "Istituzioni di diritto Pubblico" presso la Facoltà di Scienze della Comunicazione dell'Università di Roma La Sapienza; attualmente è titolare dell'insegnamento "Regolamentazione giuridica delle reti". È Coordinatore dell'Osservatorio Normativo della Rivista "Diritto dell'Internet", IPSOA Editore, e ha pubblicato più di un centinaio di articoli sulle riviste specializzate nel diritto dell'informatica e delle telecomunicazioni.

DIGITAL DIVIDE - DEFINIZIONE

La creazione e la diffusione delle nuove tecnologie dell'informazione e della comunicazione ha accelerato lo sviluppo e la crescita di alcune nazioni a scapito di altre. In questo contesto qualcuno ha segnalato l'esistenza di un paradosso che vede da un lato la presenza di nazioni "deboli" e dall'altro di nazioni "forti": l'une costrette ad affrontare il problema dell'accesso alle informazioni, le altre all'eccesso.

Al fine di evidenziare questo paradosso è stato utilizzato il termine digital divide (divario digitale) identificando nella separazione tra nazioni forti e deboli un motivo di sperequazione. Quindi la capacità di utilizzare le tecnologie dell'informazione e delle comunicazioni diventa una nuova forma di alfabetismo "digitale".

Vi sono stati numerosi dibattiti riguardo al digital divide; fra i più celebri: la dichiarazione "Millennium" dell'ONU, il G8 di Okinawa, la "carta di Bologna".

La dichiarazione del Millennio (2000): il Segretario Generale delle Nazioni Unite Kofi Annan introdusse una sezione denominata "Costruire ponti digitali": in essa si osservava l'esistenza di cambiamenti di capitale importanza che si stavano verificando nelle industrie delle comunicazioni e

dell'informazione, e che avevano iniziato a trasformare la vita economica e sociale. Kofi Annan definì questi cambiamenti la rivoluzione digitale.

La carta di Okinawa (2000): al termine del summit nacque la carta, documento sulla società globale rivolto a studiare e descrivere l'impatto dell'informazione sulla società civile. La carta è suddivisa in cinque sezioni:

- cogliere le opportunità digitali;
- superare il dislivello digitale;
- promuovere la partecipazione globale;
- andare avanti;
- le priorità.

Con la carta si riconosce anche il fatto che le politiche per l'avanzamento della Società dell'Informazione devono essere sostenute dallo sviluppo delle risorse umane in grado di rispondere alle domande dell'era dell'informazione.

Si rinnova l'impegno a fornire a tutti i cittadini un'opportunità di coltivare l'alfabetizzazione e le attitudini all'Information Technology attraverso la cultura, la formazione permanente e l'esperienza.
Si deve continuare a lavorare verso questo ambizioso fine mettendo online scuole, classi e biblioteche ed insegnanti esperti in IT e in risorse multimediali.

Durante il vertice è stata creata la DOT Force (Digital Opportunity Task), formata da 42 gruppi di rappresentanti di governi, del settore privato, di organizzazioni non-profit e di organizzazioni internazionali, che si sono uniti in uno sforzo comune volto ad individuare gli interventi necessari per far sì che la rivoluzione digitale possa generare benefici per tutti i cittadini del pianeta, soprattutto per i più poveri ed emarginati.

La carta di Bologna: le città intervenute si sono poste due obiettivi: il primo riguarda la possibilità di rafforzare e moltiplicare i risultati della politica e dell'azione nazionale ed internazionale; il secondo concerne la possibilità di contribuire alla realizzazione di competenze locali e a trasformare tutti i settori dell'economia locale.

Al fine di mobilitare i soggetti attivi nel campo dell'istruzione e della formazione nonché i protagonisti in ambito sociale, industriale ed economico, il 24/5/2000 la Commissione Europea

adottò un'iniziativa denominata e-learning, pensare all'istruzione di domani, attraverso i piani d'azione e-Europe 2002 e 2005 che fanno dell'e-learning una priorità assoluta e fissano obiettivi ambiziosi per l'infrastruttura, l'attrezzatura e la formazione di base che tale integrazione presuppone.

"Digital divide", è il termine tecnico utilizzato per le disuguaglianze nell'accesso e nell'utilizzo delle tecnologie della cosiddetta "Società dell'Informazione" [1].

Divario, disparità, disuguaglianza digitale significano in sostanza la difficoltà da parte di alcune categorie sociali o di interi paesi di usufruire di tecnologie che utilizzano una codifica dei dati di tipo digitale rispetto ad un altro tipo di codifica precedente, quella analogica.

Si distinguono tradizionalmente le problematiche del divario globale da quelle relative alle disuguaglianze in ambito interno.

Al fine di attenuare le conseguenze della diseguale distribuzione delle risorse informatiche e conseguente divario digitale, si rendono necessarie alcune politiche di riequilibrio.

DIGITAL DIVIDE E TELECOMUNICAZIONI

I principali punti per descrivere il digital divide sono, ai fini che interessano la presente ricerca sull'aspetto relativo alle telecomunicazioni:

- carenza delle infrastrutture per le telecomunicazioni ;
- costi elevati di utilizzo delle linee telefoniche [2];
- scarsa presenza di computer e attività di alfabetizzazione relative al loro utilizzo;
- diffusione geografica delle connessioni, concentrata nelle grandi città o esclusivamente nelle capitali, mentre è totalmente assente nelle zone rurali, nelle quali vive una rilevante parte della popolazione.

Quest'ultima condizione è presente anche in paesi ritenuti fortemente industrializzati, quali ad esempio l'Italia.

In generale quindi la totale inadeguatezza o l'inesistenza di mezzi di telecomunicazione sufficienti appaiono in grado di generare un circolo vizioso che genera scarsezza di "ritorni" economici certi e dunque danni ai consumatori ed alla loro possibilità di avere accesso, in condizioni paritarie, alle tecnologie dell'informazione.

DIGITAL DIVIDE E SPETTRO RADIO

Fra le soluzioni ipotizzate per risolvere il digital divide nel contesto interno, la più praticabile in termini relativamente brevi è quella di utilizzare le frequenze radio.

L'utilizzo delle frequenze, eventualmente utilizzando architetture di rete che consentano una rete basata su ponti radio, appare senz'altro un ottimo strumento per raggiungere zone disagiate (ad esempio comunità montane) che altrimenti resterebbero tagliate fuori dal resto del territorio a causa dei meccanismi di business degli operatori di telecomunicazioni.

Fra le proposte concrete per eliminare il digital divide si segnalano le iniziative di "spettro" libero che sarebbero in grado di creare le condizioni per un'accelerata alfabetizzazione digitale, rendendo disponibili alla collettività frequenze radio liberamente sfruttabili per comunicare, anziché attribuire con strumenti di gara le stesse frequenze ad uno o più operatori economici in grado di sfruttarle.

Una prima "liberalizzazione" delle frequenze sembra essere stata utilizzata con le reti c.d. wi-fi, che però scontano la scarsa potenza degli apparati e dunque l'impossibilità di realizzare reti complesse in grado di servire comunità più o meno ampie di cittadini [3].

Sulla falsariga dell'utilizzo delle frequenze libere e condivise tipiche del wi-fi e di esperienze estere di connettività, fornita direttamente dagli organi istituzionali (come quelle della città di San Francisco o Saint Louis negli Stati Uniti e Amsterdam in Olanda), si è sviluppato un dibattito sull'utilizzo libero delle frequenze relative al Wi Max , al fine di favorire gli utenti e di concedere loro il diritto di poter utilizzare liberamente frequenze ed apparati [4].

Fra i fautori di un utilizzo libero delle frequenze (con particolare riferimento alle emanande licenze relative al Wi Max), vi è il Capitolo Italiano di Internet Society (ISOC) che si è fatto capofila delle iniziative "libertarie" sorte negli scorsi mesi in Italia [5].

Il punto nodale dell'intera vicenda è stato quello relativo ad un uso delle frequenze compatibile con i principi di libera circolazione del sapere, propria dell'open source, e i principi di limitazione proprietaria delle frequenze tipica di alcuni istituti precedenti.

Va detto in verità che, al di là di alcune affermazioni di principio di soggetti anche autorevoli (ad esempio l'Ex Presidente della Federal Commission), quasi tutti i Paesi di fronte al dilemma di rendere libere le frequenze o ricavarne comunque un introito hanno scelto la seconda soluzione, in considerazione anche del fatto che spesso le frequenze utilizzate per scopi civili provengono dalle dotazioni frequenziali dei militari e questi ultimi in genere chiedono una contropartita per il rilascio delle frequenze.

La possibilità tuttavia di lasciare alla libera disponibilità degli utenti le frequenze (o parte di esse) potrebbe effettivamente essere esplorata in quelle zone non attraenti dal punto di vista commerciale, ovvero le zone particolarmente non appetibili e affette dal digital divide.

Per analizzare le ragioni dei fautori del libero spettro bisogna comprendere i motivi che questi ultimi ritengono fondamentali: il presupposto da cui sostanzialmente partono i fautori del libero spettro è che quest'ultimo non possa qualificarsi come risorsa scarsa.

In base a questa teoria, una regolamentazione dello spettro in termini proprietari contrasterebbe con l'utilità sociale [6].

Inoltre un utilizzo in termini di capacità trasmissiva efficiente da parte degli utenti, anziché una allocazione a seguito di selezione pubblica costituirebbe il presupposto di un uso condiviso ed efficiente delle frequenze.

Il presupposto alla base di questa teoria è che la limitatezza dello spetto, e quindi l'esigenza di ripartirlo nel contesto digitale, sia in verità un paravento in grado di perpetuare (o creare) condizioni di sfruttamento da parte di alcuni soggetti.

Ma è proprio così?

Per comprendere se un originario sistema libero sia effettivamente in grado di creare le condizioni per un uso condiviso, occorrerebbe forse soffermarsi sulla storia recente delle radiofrequenze per comprendere quello che potrebbe accadere anche al Wi Max.

Prendiamo ad esempio ciò che è accaduto in Italia con la deregolamentazione delle frequenze nel settore radiotelevisivo che ha avuto origine negli anni '70 con la sentenza RAI; a questa sentenza ha

fatto seguito un periodo di grande confusione, a cui diversi provvedimenti hanno tentato di dare una soluzione, fra i quali la sentenza della Corte Cost. n. 102/1990 che ha stabilito che l'esercizio di impianti radiotelevisivi comporta l'utilizzazione di un bene comune - l'etere - naturalmente limitato, rendendo così necessario un provvedimento di assegnazione della banda di frequenza. In sostanza, nel mondo radiotelevisivo, la libertà conseguente alla deregolamentazione e all'apertura delle frequenze ha generato un vero e proprio "far west" all'interno del quale, e sino a tempi recenti, si è affermata la pratica dell'occupazione" delle frequenze, delle interferenze, dei "ricatti" delle più forti nei confronti delle più deboli, attuati ad esempio con l'aumento della potenza degli apparati a danno delle radio più piccole.

Questo stato di cose è divenuto per un certo periodo la prassi, ed anche oggi che vige una regolamentazione più stringente, i rapporti tra i titolari delle frequenze, fra emittenti nazionali e locali è spesso regolato da accordi più o meno informali.

Accordi che sono egemonizzati dai più forti, a danno dei più deboli, che sono sempre esposti alle "ritorsioni" o alle occupazioni di chi illecitamente aumenta la potenza degli apparati, oscurando i rispettivi legittimi ambiti di trasmissione. Fra gli altri risultati di una liberalizzazione senza controllo, conseguente all'entusiasmo per la agognata liberalizzazione delle frequenze, vi è stata la creazione di gruppi di potere molto concentrati tale da creare un abisso tra i gruppi editoriali che sono espressione di holding dell'informazione e le radio che una volta si sarebbero chiamate "libere" che difficilmente riescono a sostenere gli oneri economici delle trasmissioni.

Ulteriore corollario di questo stato di cose è l'ipervalutazione in termini economici delle frequenze, una volta "libere".

Anche nel mondo televisivo l'iniziale "latitanza" del diritto, conseguente alla già citata liberalizzazione, ha portato al giorno d'oggi a situazioni difficili da definire in termini giuridici ed alla creazione di un mercato fortemente concentrato.

Esemplare in tal senso è il c.d. principio dell'assentimento, contenuto nella c.d. legge Gasparri, ovvero il principio in base al quale, in presenza di una situazione di duopolio televisivo, il legislatore si è limitato a registrare la realtà consolidata nel tempo.

Il principio dell'assentimento non è altro che l'affermazione del principio res sic stantibus ovvero stando così le cose lo Stato registra, come fosse un notaio, la situazione attuale dandole veste giuridica.

Chi ha avuto la forza economica e giuridica per emergere dal far west iniziale si tiene le frequenze e ha anche la capacità di scacciarne altri, perpetuando in tal modo una situazione di concentrazione anticoncorrenziale, come ha ben chiarito l'AGCOM al termine dell'analisi di mercato sul mercato radiotelevisivo.

Orbene, la storia delle frequenze nel settore radiotelevisivo associata all'osservazione della realtà conseguente alla "liberazione delle frequenze wi fi", potrebbero assomigliare a quello che diverrebbe il fenomeno "Wi Max" qualora fosse accolta la tesi, senz'altro affascinante dell'open spectrum, anche se il principio di base da cui partire, ovvero l'eliminazione del digital divide, è senz'altro condivisibile. In proposito, basta osservare la realtà italiana di questi ultimi due anni.

Chi conosce veramente la materia sa cosa può accadere se più persone contemporaneamente decidono di creare più reti operanti sulla stessa frequenza non licenziata. Se tra queste reti ve ne è una ad esempio di un ente pubblico o di una grande realtà operativa nel settore delle telecomunicazioni, difficilmente qualcun altro nelle vicinanze riuscirà a ricevere o a trasmettere, così come un soggetto con una stazione base collocata in cima ad una montagna riuscirà ad impedire facilmente la trasmissione di una stazione base di un concorrente che ne ha un'altra in un'area metropolitana in fondo alla valle.

I fautori dell'open spectrum ritengono che il libero uso sia in grado di premiare chi è in grado di sfruttare la capacità trasmissiva, sia esso un semplice cittadino oppure un impresa, determinando in tale modo la massimizzazione dell'utilità del sociale che si porrebbe in funzione preminente rispetto al profitto.

Il risultato si otterrebbe concedendo a "chiunque" il beneficio dell'utilizzo dello spettro.

È facile osservare che, tra i "chiunque", ci possa essere senz'altro chi avrà la forza economica-giuridica e fattuale per escluderne altri, attuando comportamenti opportunistici a danno della collettività e a fini (opportunamente mascherati") di massimizzazione del profitto.

Non è dunque la scarsità di frequenze a determinare il conflitto ma la posizione di potere, in assenza di regole certe preventive, di chi è in grado di influenzare gli andamenti della tecnologia.

Questo processo, che ha accompagnato la crescita delle telecomunicazioni in Italia e che ha determinato fra le altre conseguenze la nascita di zone digital-divise nel nostro Paese, è sostenuto da diversi fattori trainanti tra i quali senz'altro vi sono quelle che vengono chiamate l'asimmetria informativa e di posizione.

Si parla di una situazione di informazione asimmetrica quando una delle parti, in una relazione economica, dispone di maggiori informazioni rispetto alla controparte sulle proprie caratteristiche o sulle azioni intraprese o sull'ambiente esterno, elementi che incidono sui risultati della relazione e quindi sul benessere dei partecipanti.

L'asimmetria informativa nel settore del Wi Max avrebbe due principali fattori, uno senz'altro qualificabile come positivo, l'altro invece negativo, che potrebbero essere colmati dallo Stato:

1. il primo riguarderebbe lo Stato il quale, non avendo informazioni certe sul mercato delle frequenze, potrà disporre di un processo di selezione del contraente privato che gli consenta di comprendere il valore delle frequenze;
2. il secondo riguarderebbe i soggetti economici non in grado di essere competitivi per via delle economie di scala dei grandi gruppi economici.

Quest'ultima situazione di debolezza, qualora lo spettro sia liberamente a disposizione di chi abbia la capacità di sfruttarlo, potrebbe essere perpetuata in seguito da una regolamentazione che certifichi gli equilibri esistenti, analogamente a ciò che è avvenuto nel mondo della radiotelevisione.

In sostanza potrebbe accadere che nel prossimo futuro venga emessa una norma che si limiti a "fotografare" la realtà esistente ed a legittimare la posizione dei soggetti che, per forza economica o per altri fattori, sono emersi come protagonisti del settore Wi Max, occupando le frequenze .

Ed è per questo motivo che uno spettro totalmente libero, fonte di potenziali conflitti, al di là dei potenziali miglioramenti che il contesto digitale può realizzare, non possa essere praticabile in determinati contesti, dovendo necessariamente lo stato assumere un ruolo di regolatore dei meccanismi economici alla base della convivenza civile.

Ed è ancora per questo motivo che lo Stato ha l'obbligo di intervenire per tutelare le posizioni dei soggetti più deboli, siano essi i semplici cittadini o le imprese in posizione subalterna rispetto a coloro che detengono il potere, predisponendo ad esempio una normativa contenente misure asimmetriche a carico delle imprese in posizione dominante, quali ad esempio l'ingresso ritardato di alcuni operatori nel mercato o l'obbligo di copertura di determinate zone svantaggiate.

Peraltro l'intervento dello Stato, espressamente previsto nella ricostruzione teorica di Pareto, diviene necessario allorquando, nella realtà dei mercati, prevalgono situazioni di concorrenza imperfetta o monopolistica o di oligopolio. Tutte situazioni attualmente presenti nel settore delle comunicazioni in Italia.

In tutte queste situazioni effettive di mercato, viene violata la condizione di uguaglianza fra prezzo e costo marginale che realizza l'equilibrio delle imprese in concorrenza perfetta e che, per il 1° teorema dell'economia del benessere, quando siano soddisfatte le altre condizioni richieste dal teorema stesso, assicura l'ottimo paretiano.

Alcuni autori (in contesti del tutto differenti peraltro) hanno effettivamente ritenuto che la norma dovesse seguire e non precedere né orientare in alcun modo la tecnologia; ciò è senz'altro vero in diversi ambiti ma non in quelli delle radiofrequenze, come dimostra la storia del settore radiotelevisivo, per i rischi in termini di chiusura del mercato e di pericoli ai diritti costituzionali dei cittadini.

La presenza dello Stato come regolatore dei processi di diffusione delle tecnologie dell'informazione si colloca, come è noto, all'estremo della teoria dello sfruttamento libero delle risorse, in quanto prevede un ruolo proattivo della Comunità nazionale, al fine di prevenire o evitare la nascita di zone digital divise.

Fra le ipotesi che si sono affacciate ve ne sono alcune che privilegiano l'intervento "mediato" dello Stato nello sviluppo delle reti di telecomunicazioni in Italia, attraverso la creazione di società a partecipazione pubblica in grado di investire nelle zone digital-divise.

Questa impostazione deriva direttamente dalla constatazione che la libera concorrenza, in alcune zone depresse dal punto di vista commerciale, non porta ai benefici attesi, al punto di acutizzare, anziché diminuire, le conseguenze del digital divide.

Tuttavia il massiccio ricorso agli strumenti pubblico-privati sarebbe idoneo, in alcuni casi, a creare delle distorsioni notevoli della concorrenza privando le realtà commerciali medio-piccole della possibilità di creare innovazione nelle zone colpite anche da problemi endemici quali la disoccupazione, sottraendo anche al controllo dello Stato, come è avvenuto nel caso dei c.d. affidamenti in house, al controllo dello Stato e degli organi di controllo giurisdizionale, l'assegnazione di fondi pubblici [7].

DIGITAL DIVIDE E BANDA LARGA: IL SERVIZIO UNIVERSALE PERVASIVO

Secondo alcune correnti di pensiero [8] il superamento del digital divide interno deve essere una questione affidata all'intervento pubblico perché solo questo potrebbe contribuire a ridurlo nel breve-medio termine, creando delle infrastrutture di connettività per portare la banda larga, ma non solo [9].

Secondo altri Autori invece esiste una criticità nell'ipotizzare un possibile intervento pubblico volto ad equilibrare i meccanismi del mercato; infatti la diffusione di massa delle tecnologie informatiche dovrebbe essere conseguita gradualmente, grazie alla riduzione dei prezzi dovuta alla liberalizzazione del mercato delle telecomunicazioni, e dovrebbe compiersi coinvolgendo quote sempre maggiori di popolazione [10].

Inoltre coloro che guardano con "sospetto" all'intervento statale per l'eliminazione del digital divide temono che tale intervento possa stimolare la propensione mostrata dai governi a controllare e regolamentare quello che circola sulla rete, oltre a gravare il bilancio dello Stato di oneri economici non indifferenti per dotare delle necessarie infrastrutture tutte le aree che ancora ne sono prive [11].

La prima impostazione viene seguita da alcuni Paesi che sembrano aver individuato nell'obbligo di fornitura dei collegamenti a banda larga, secondo i modelli tipici del c.d. Servizio Universale, le condizioni per uno sviluppo delle reti di telecomunicazioni in modalità egualitaria e tale da consentire a tutti i cittadini di poter avere accesso in condizioni paritarie alle tecnologie dell'informazione [12].

Il Servizio Universale comprende un'offerta di base di servizi di telecomunicazione che devono essere offerti su scala nazionale a tutte le categorie della popolazione, con un buon livello di qualità

a prezzi convenienti. Questi servizi di base sono ad esempio il servizio telefonico pubblico, il servizio di trasmissione dati, l'accesso ai servizi d'emergenza, un numero sufficiente di cabine telefoniche pubbliche o servizi speciali per audiolesi e ipovedenti. Con il Servizio Universale, il legislatore vuole evitare che regioni periferiche o gruppi di persone siano svantaggiati.

Peraltro il nostro legislatore, pur menzionando l'accesso ad Internet negli articoli del Codice delle Comunicazioni Elettroniche relativi al servizio universale, non ne prevede l'inclusione obbligatoria.

In base all'articolo 54 dello stesso Codice, "qualsiasi richiesta ragionevole di connessione in postazione fissa alla rete telefonica pubblica e di accesso da parte degli utenti finali ai servizi telefonici accessibili al pubblico in postazione fissa è soddisfatta quanto meno da un operatore. La connessione consente agli utenti finali di effettuare e ricevere chiamate telefoniche locali, nazionali ed internazionali, facsimile e trasmissione di dati, e deve essere tale da consentire un efficace accesso ad Internet."

La norma, come è agevole rilevare, non prevede a carico degli operatori obbligati alla fornitura del Servizio Universale, l'obbligo di ricomprendere, al proprio interno, anche i collegamenti a banda larga, e tale esclusione determina ovviamente che, su base volontaristica, nessun operatore fornisca a prezzi calmierati e controllati l'accesso ad Internet in zone non appetibili commercialmente.

Va detto che la concezione secondo la quale Internet rientrerebbe tra gli obblighi facenti parte del c.d. Servizio Universale sembra essere esclusa, in linea di principio anche dalle Istituzioni Comunitarie.

La Commissione Europea, per ammissione del Commissario Viviane Reding, ha preso una posizione estremamente netta nel 2006 escludendo che le connessioni bradband e le comunicazioni mobili potessero entrare a far parte della famiglia dei Servizi Universali, tranne che nei casi nei quali vi siano particolari problemi strutturali, quali l'isolamento geografico che consentano l'impiego di investimenti pubblici per ridurre il divario digitale.

Una soluzione diversa da quanto invece realizzato in Svizzera, laddove la Commissione federale delle comunicazioni, alla fine di giugno del 2007, ha designato l'operatore Swisscom quale "concessionario del Servizio Universale" a partire dal 2008.

Secondo la Commissione federale delle comunicazioni, per i prossimi dieci anni la compagnia "sarà dunque tenuta a fornire le prestazioni del Servizio Universale in materia di telecomunicazioni all'insieme della popolazione e in tutte le regioni del Paese. La nuova concessione obbliga Swisscom a offrire, oltre al collegamento analogico e digitale, anche una connessione Internet a banda larga".

"Il Servizio Universale in Svizzera - spiega la stessa Commissione - include ora anche la messa a disposizione di un collegamento a Internet a banda larga con una velocità di trasmissione pari a 600/100 kbit/s; si tratta di una prima mondiale" [13]. Ai tipi di collegamento telefonico attualmente contemplati nel Servizio Universale, ne verrà quindi aggiunto uno nuovo che permette una connessione a Internet ad alta velocità.

Va detto che anche in Italia (sino ad oggi peraltro senza particolare attenzione da parte delle Istituzioni) sono ormai molti anni che utenti e consumatori (ma anche Associazioni di imprese, che sperano in tal modo di abbattere la posizione oligopolistica di fatto degli operatori dominanti) si battono affinché la fornitura di ADSL, o comunque di connettività broadband, sia considerata un Servizio Universale.

NOTE

[1] Il termine digital divide viene utilizzato per la prima volta nel 1995, quando la National Telecommunications and Information Administration (NTIA) , organo consultivo degli Stati Uniti sulle politiche nel settore delle telecomunicazioni, pubblica la relazione “A Survey of the “Have nots” in Rural and Urban America”, la prima di una serie intitolata “Falling Trought the Net”. www.ntia.doc.gov

[2] L’importanza delle reti di telecomunicazione come prerequisito delle condizioni di sviluppo delle reti digitali è colta felicemente da Ferri, “La rivoluzione digitale”, Milano, 1999. In tema anche Norris, “Digital divide, civic engagement, information poverty and the internet worldwide”, Cambridge, 2001, Cambridge university press; Buongiovanni, Marzano, Tesi, Zocchi, “Digital divide”, Franco Angeli 2003; Carbone e Guandalini “Vendo capre su Internet: e-economy e digital divide: breve itinerario lungo le nuove frontiere dell’on-line”, Milano, Etas 2002; Carlini, “Divergenze digitali. Conflitti, soggetti e tecnologie della terza Internet”, 2002 Roma, Manifestolibri.

[3] In generale sulle reti wireless: Gast, "802.11 “Wireless Networks: The Definitive Guide”, Linux Journal, Maggio 2002; "The answer to the WLAN vs 3G argument", Wireless World Forum, Febbraio 2002; Corrias, "wi-fi, l'unione fa la rete”, Interpuntonet no.81, Luglio/Agosto 2002, pp. 8-14; Di Lullo, "wi-fi-nuova frontiera wireless" (Disponibile al sito: http://www.geocities.com/SiliconValley/Garage/1748/wifi /); Trani, “Le comunicazioni Wireless: analisi del segmento di mercato”, 2002. (Disponibile all’indirizzo: http://www.rdn.it/it/wireless/wirele.htm)

[4] 4 Si vedano le interessanti osservazioni di Manfredini, “San Francisco, e Roma china il capo”, in Punto Informatico del 25 ottobre 2004. Peraltro, nel gennaio 2007, le Società Google ed Earthlink si sono aggiudicate la gara per realizzare una rete wi-fi nella città californiana. Secondo le specifiche fornite dalle due Società, il servizio sarà fruibile entro il 2008 nell’intero territorio della città. Google, che ha già realizzato una rete wi-fi nella «sua» Mountain View, offrirà una connessione gratuita, e pubblicizzata, alla velocità di 300 kb al secondo. Chi vorrà «viaggiare» più velocemente, e senza pubblicità, potrà abbonarsi invece al servizio di Earthlink, offerto a 21,95 dollari al mese. Prezzi inferiori per coloro che hanno bassi redditi, proprio con l'obiettivo - sostiene l'amministrazione locale - di garantire davvero Internet per tutti.

[5] Posizione di ISOC Italia in merito all'introduzione della tecnologia Wi Max in Italia 5 Marzo 2007

[6] Questa impostazione è stata prescelta in Italia da diversi Autori, primo fra tutti Favara Pedarsi , “Wi Max l’Italia lo sta depotenziando”, in Punto Informatico del 19 febbraio 2007.

[7] Bertini, “Fattori di successo e condizioni di sviluppo delle piccole e medie imprese”, Giappichelli,Torino 1995; Brugnoli, “La nuova impresa innovativa”, Giappichelli,Torino 2003.

[8] In generale, sul Servizio Universale: Castelli, “Il Servizio Universale nelle telecomunicazioni”, Milano, Franco Angeli Editore, 1997; Ravazzi, Valletti, “Le telecomunicazioni in Gran Bretagna”, Politica Economica, vol. 15, n. 3, 1999; Radicati Di Brozolo, “Il diritto comunitario delle telecomunicazioni”, Torino, Giappichelli, 1999; Venturini, “Servizi di telecomunicazione e concorrenza nel diritto internazionale e comunitario”, Torino, Giappichelli, 1999; Cremer, Gasmi, Grimaud e Laffont, “The Economics of Universal Service: Theory”, The Economic Development Institute of the World Bank, 1998; Cremer, Gasmi, Grimaud e Laffont, “The Economics of

Universal Service: Practice", The Economic Development Institute of the World Bank, 1998; Gasmi, Laffont, Sharkey, "Competition Policy and Universal Service", Settembre 1998; Weller, "Auctions for Universal Service Obligations", Presented at the twelfth biennal conference of the ITS, Stoccolma, Giugno 1998; Prieger, "Universal Service and the Telecommunications" Act of 1996 - The fact after the act, Telecommunications Policy, Vol. 22, No. 1, pp. 57-71, 1998; Michael Noll, "The costs of competition - FCC Telecommunication Orders of 1997, Telecommunications Policy", Vol. 22, No. 1, pp. 47-56, 1998

[9] Buongiovanni, Marzano, Tesi, Zocchi "digital divide" già citato.

[10] Peraltro la possibilità di includere l'accesso ad Internet tra gli obblighi relativi al Servizio Universale è stata oggetto di controverse prese di posizione anche da parte delle Istituzioni Statunitensi : nel 1996, nell'ambito del procedimento di consultazione che ha portato all'emissione del c.d. Universal Service Order, la FCC ha ritenuto che quanto all'accesso ad Internet, questo non dovesse rientrare nei servizi garantiti nell'ambito della fornitura del Servizio Universale trattandosi di un servizio di informazione e non di telecomunicazione.

[11] Carlini, "Internet, pinocchio e il gendarme. Le prospettive della democrazia in rete", 1996, Roma, Manifestolibri, pp. 128-130.

[12] Peraltro l'idea non è nuova in Italia già nel 1997 Manlio Cammarata , nella rivista Interlex parlava di Internet e Servizio Universale: Cammarata, "Internet come Servizio Universale: una battaglia da vincere", 09.12.97 http://www.interlex.it/tlc/mcservun.htm

[13] Si veda il commento di Bonacina, "Svizzera, là dove l'ADSL è un diritto di tutti", in Punto Informatico del 25 giugno 2007.

APPENDICE: INTERNET GOVERNANCE FORUM

A CURA DI

LAURA ABBA E CARLO N. COSMATOS

Laura Abba, laureata in Matematica, dirigente del CNR , è membro del Comitato che accompagna il Governo italiano nella predisposizione delle linee di azione italiane sulle grandi tematiche di Internet. Attività centrata sul supporto alle interazioni istituzionali fra le Reti telematiche per la Ricerca e la Rete Internet. Partecipa fin dall'inizio ai progetti che hanno introdotto Internet in Italia collaborando, anche in ambito GARR, alla realizzazione delle reti per la ricerca e allo sviluppo della società dell'informazione. Cura l'impianto del primo corso Internet TCP/IP tenuto in Italia (Scuola Sant'Anna, Pisa, ottobre 1991) a titolo "Le reti per la ricerca scientifica protocolli ed applicazioni TCP/IP" e da allora opera con continuità alla distribuzione di cultura e tecnologie INTERNET: è membro dei comitati organizzativi, tecnici, scientifici, di numerosi eventi dedicati; è autore di numerose pubblicazione e rapporti tecnici. Eletta nel 2003 al Consiglio Direttivo di Società Internet (capitolo italiano della Internet Society) cura per ISOC Italia la linea editoriale dell'associazione.

Carlo N. Cosmatos, nato nel 1968 si è laureato in Scienze Politiche all'Università di Pisa, sin da giovane radioamatore, grande passione per le telecomunicazioni, si è impegnato su temi della rete Internet sin dal 1994, realizzando uno dei primi siti/blog dedicati al commercio elettronico. Progetto realizzato interamente per sua capacità personale, segnalato da governi, pubbliche amministrazioni e dal settore privato, dopo quasi 10 anni di attività continua ad essere tra i principali punti di riferimento sul commercio elettronico inteso nei suoi vari aspetti (http://commercioelettronico.freeunixhost.com/). Ha lavorato ad Atene per la STET Hellas, ed opera come freelance nel mondo dell'e-business. Membro attivo della Società Internet ISOC Italia, collabora con l'Istituto Internazionale di Studi e formazione su Governo e Società (www.iiefgs.org) promosso dalle Università di Pisa e Salvador a Buenos Aires, come curatore del programma "Tecnologie e Politiche per la Società dell'Informazione". Dalla fine del 2006 cura lo sviluppo del sito web di ISOC Italia.

Presentiamo un riassunto dei lavori che si sono svolti nelle principali sessioni del primo IGF Forum di Atene. Il nostro contributo ha lo scopo di far conoscere agli utenti italiani della rete alcune problematiche emerse, che rappresentano la base di partenza per gli impegni del prossimo IGF Forum di Rio.

PREMESSA

Promosso dalle Nazioni Unite, il secondo Internet Governance Forum (IGF) [1] si svolgerà a Rio de Janeiro dal 12 al 15 Novembre prossimo, un'importante opportunità per il popolo della rete alla

ricerca di un benessere universale fondato sullo strumento Internet. La partecipazione è aperta a tutti coloro che sono interessati alla conoscenza e allo sviluppo della rete Internet.

La creazione dell'IGF è stata uno dei risultati più significativi dell'ultimo World Summit On Information Society (WSIS) [2], tenutosi a Tunisi dal 16 al 18 Novembre 2005. L'Agenda [3] di Tunisi per la Società dell'Informazione ha sottolineato l'importanza di attivare un nuovo Forum 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. Il meeting inaugurale dell'IGF è stato un successo e si è svolto nel Novembre 2006 ad Atene. Dopo Rio, l'IGF si terrà a Nuova Delhi nel 2008, a Il Cairo nel 2009 e a Vilnius o Baku nel 2010.

Il Forum è aperto a tutti, secondo i principi del multilateralismo, multi-stakeholder, di democrazia e trasparenza [4]. I ruoli e le responsabilità degli stakeholder, suddivisi in tre categorie – Governi, Settore Privato e Società Civile - sono stati definiti dal Rapporto [5] del WGIG del luglio 2005. La missione [6] del Forum è quella di facilitare le discussioni e lo scambio di esperienze sulle questioni di politica pubblica relative ai fattori chiave dell'Internet governance [7]. Il Segretario Nazionale delle Nazioni Unite, Ban Ki-moon, nella sua lettera d'invito per Rio, richiama l'attenzione sull'importanza dell'assistenza ai paesi in via di sviluppo: « ... second Forum should build on the success of Athens, and retain its overall theme of "Internet Governance for Development"....». Ricordiamo che il ruolo delle Nazioni Unite è esclusivamente quello di promotore e facilitatore degli incontri previsti.

L'IGF è un organismo privo di poteri decisionali che mira a facilitare il dialogo tra tutte le parti interessate (stakeholders) sullo sviluppo del sistema Internet, favorendo altresì la creazione di cosiddette "coalizioni dinamiche", ossia gruppi di lavoro aperti informali che si attivano per elaborare proposte sui singoli argomenti. Tali proposte saranno poi portate all'attenzione dei partecipanti del Forum. Una loro eventuale adozione sarà sempre e comunque 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, istituzioni o organizzazioni [8], ma può eventualmente emanare Raccomandazioni elaborate con il contributo degli utenti della rete.

Durante il processo di preparazione per il prossimo Forum di Rio si è convenuto che esso avrà come temi principali i quattro del primo meeting di Atene: – OPENNESS", SECURITY", DIVERSITY," ACCESS – con l'aggiunta di un quinto tema: CRITIC RESOURCES.

Il meeting di Atene [9] si è svolto a Vouliagmeni, una località a 30 chilometri dalla capitale greca. Le organizzazioni di oltre 97 paesi del mondo, con 397 delegazioni, 1350 iscritti e oltre 150 giornalisti si sono confrontate partecipando nelle sei sessioni plenarie. Le trascrizioni come il web cast di tutte le sessioni sono disponibili in rete.

Openness	intgovforum.org/IGF-Panel2-311006am.txt
Security	intgovforum.org/IGF-Panel3-311006.txt
Diversity	intgovforum.org/IGF-SummingUp-011106.txt
Access	intgovforum.org/IGF-Panel5-011106.txt
Emerging Issues	www.intgovforum.org/IGF-Panel6-021106.txt
The way forward	www.intgovforum.org/IGF-SummingUp2-021106am.txt

In parallelo alle sessioni plenarie si sono svolti i workshop, dedicati a specifiche problematiche della Internet governance.

Il Governo italiano[10], in collaborazione con ISOC ITALIA, Ip Justice (USA) e il Centro per la Tecnologia e la Società Getulio Bargas (Br), ha proposto ad Atene, con successo, un coalizione dinamica sulla Carta dei diritti degli utenti della rete dal nome “Bill of rights”.

Bill of rights	www.internet-bill-of-rights.org/
Spam	www.stopspamalliance.org
Privacy	*sito in allestimento*
Standards Aperti	igf-dcos.org
Accesso alla conoscenza (A2K) e Libertà di Espressione	www.a2k-igf.org
Libertà di espressione e Libertà dei media in Internet	www.foeonline.wordpress.com
Accesso e Connettività delle aree rurali	www.pacificit.org/dc
Diversità Linguistica	www.maayajo.org

Le Coalizioni Dinamiche sono delle coalizioni informali che riuniscono organizzazioni che si impegnano ad affrontare in comune la risoluzione di determinate problematiche, e costituiscono un

risultato importante del primo IGF. Le altre Coalizioni Dinamiche che si sono formate ad Atene riguardano le tematiche in tabella.

Grazie a tutte queste sinergie che si sono attivate e al nuovo modus universale di dialogo intrapreso, il primo IGF ha avuto un grande successo.

IL PRIMO INTERNET GOVERNANCE FORUM, ATENE 2006

In alcuni paesi, la via per Atene è stata preparata tramite la organizzazione di eventi pre IGF Forum a livello nazionale. Questi incontri preparatori si sono rilevati importanti ai fini della comprensione degli interessi particolari che preoccupano i singoli stati nazionali.

Il Governo italiano ha risposto alla iniziativa dell'IGF fin dall'inizio. Il Ministro Luigi Nicolais ha avviato il 3 agosto 2006 i lavori di un Comitato, costituito da otto tra i massimi esperti di Internet, per accompagnare il Ministro e il Governo nella predisposizione delle linee di azione italiane. ll Comitato [11] è coordinato dal Professore Stefano Rodotà ed ha come riferimento diretto il Sottosegretario Beatrice Magnolfi. Prima di Atene, il 12 ottobre 2006, si è tenuta una Assise pubblica a Roma, ove i politici si sono presentati con la piena volontà nell'intraprendere un percorso di comprensione sulle problematiche tecnologiche, affidandosi a tecnici ed esperti in grado di guidarli nel processo decisionale, ed ascoltando la società civile e l'utente individuale, anche tramite il Forum on-line [12], che ha visto la partecipazione numerosa degli internauti italiani.

Durante l'apertura dei lavori l'Ambasciatore Nitin Desai (Co-Chairmen dell'Advisory Group) ha auspicato che il Forum sia innovativo quanto innovativa è la rete Internet, e che sia il segno precursore di un nuovo tipo di multilateralismo che metterà insieme diverse categorie di utenti e operatori della rete intorno allo stesso tavolo.

In seguito Nitin Desai ha letto il comunicato del Segretario Generale delle Nazioni Unite, non presente alla cerimonia. Il S.G. ha messo subito in rilevanza il ruolo che ha il Forum come veicolo di un dialogo multistakeholder; sottolineando l'importanza che deve avere il Forum nell'assistere i paesi in via di sviluppo. Il Forum costituisce la sfida di portare a confronto due culture, quella di carattere non governativa, con un processo decisionale informale dal basso verso l'alto tipico della rete Internet, rispetto alla struttura formale dei governi e delle organizzazioni non governative. Lo spirito del Forum deve essere fondato sulla cooperazione volontaria e non su vincoli di carattere legale.

Appena iniziati i lavori ad Atene, le maggiori problematiche sono state evidenziate: i diritti umani, il digital divide e la necessità di sostegno ai paesi in via di sviluppo. Sono subito affiorate anche le divergenze, tra chi preferisce lo status quo, e chi invece vuole procedere in un modo più incisivo, per cui il ruolo del Forum stesso è stato messo in discussione. Mentre sarebbe possibile per il Forum emanare “Raccomandazioni” sulle tematiche discusse, si è preferito non fare riferimento per ora a questa possibilità. L'agenda stessa del Forum è stata criticata, in quanto ha dato priorità ai problemi più legati ai quei paesi ove la penetrazione della Rete Internet è maggiore.

Sempre in apertura del Forum di Atene, si è parlato dell'arresto di un blogger greco, mentre le autorità greche parlavano della libertà di espressione. Fatto molto sconcertante che dimostra l'ambiguità dei politici nell'affrontare le tematiche della rete Internet. In modo diretto o indiretto sono emerse anche le divergenze nell'ambito dei stessi gruppi d'interesse, mettendo in alcuni casi in discussione anche la tripartizione degli stakeholder.

Si è sentita la necessità di migliorare la capacità di dialogo tra i partecipanti al Forum. Aspetto di carattere psicologico, che si scontra anche con la nostra, ovvia, ignoranza sugli usi e costumi dei popoli rappresentati. Dobbiamo iniziare ad abituarci a una stretta convivenza di carattere universale, ove sarà molto difficile relazionarsi con tante culture senza conoscerle, cercando di mantenere un comportamento di reciproco rispetto. Questo problema sarà decisamente amplificato dal multilinguismo nella rete, ove parole dal contenuto eticamente corretto per certi gruppi possono risultare offensive per altri.

Sin dal primo giorno è stato messo in rilevanza anche il problema del Internationalized domain name (IDN) [13], che ha visto contrapposti i sostenitori della soluzione come elemento fondamentale della DIVERSITY, rispetto a coloro che hanno sostenuto che gli IDN sono solo degli identificatori, e che non rappresentano l'identità culturale dei popoli. Rimane un problema di carattere linguistico e non strettamente di carattere tecnologico, come ha affermato Vint Cerf – Chair del Board di ICANN - durante il Forum.

«Noi siamo pronti» [14]. Con questa frase Beatrice Magnolfi, Sottosegretario di Stato per le Riforme e le Innovazioni nella pubblica amministrazione del governo italiano, ha avviato il suo intervento presso l’Internet Governance Forum di Atene.

«L’Italia ha grandi aspettative nei confronti del Forum di Atene. Dopo i lavori delle scorse edizioni dei World Summit on Information Society (WSIS) di Ginevra e di Tunisi, siamo pronti – ha sottolineato Beatrice Magnolfi - per lavorare alla definizione delle linee d’azione per la governance di Internet. Il nostro Paese è stato tra l’altro uno dei pochi a prepararsi ai lavori di Atene organizzando una innovativa consultazione pubblica aperta a tutta la società civile».

“L’approccio multistakeholder – ha affermato Beatrice Magnolfi – è un metodo in cui noi crediamo molto. Internet deve appartenere a tutti e la definizione della sua governance non può prescindere da un metodo democratico, inclusivo e centrato sui suoi utenti.”

Oltre a porre con forza una questione di metodo, ad Atene la delegazione italiana ha organizzato un workshop, coordinato da Stefano Rodotà, dal titolo “The Internet Bill of Rights” ed ha offerto la propria disponibilità ad organizzare un confronto a livello internazionale.

«La chiave essenziale nell'introduzione di Rodotà è consistita nella considerazione della necessità di una definizione pubblica dei diritti degli internauti, altrimenti Internet non sarà uno spazio libero oltre le leggi, queste piuttosto verranno fatte dalle corporation e dai singoli governi» - scrive Fiorello Cortiana nel suo report [15] - «Rodotà ha ricordato come Internet costituisca lo spazio pubblico più ampio e partecipato mai conosciuto dall'umanità, per questo occorre una ridefinizione dei diritti già affermati in relazione con la rete e le sue prerogative, inedite ed originali ad un tempo. Per questo occorrono sia l'uso e l'adeguamento di strumenti quali i Protocolli tra Stati sotto l'egida dell'ONU, sia strumenti impegnativi "Bind" concordati tra imprese, sia Risoluzioni e Carte dei Diritti approvati da organismi sovranazionali cui fanno riferimento aree regionali del pianeta, come l'Europa ed il suo Parlamento e il Mercosur in America Latina».

Rispettando l’impegno preso in Atene, il Governo italiano in collaborazione con il Segretariato dell’IGF, Nitin Desai, sta organizzando l’evento dal titolo “Dialogue Forum on Internet Rights” previsto per il 27 settembre 2007, presso la sala della Protomoteca del Palazzo del Campidoglio in Roma. Lo scopo è quello di raggiungere i seguenti obiettivi: 1) contribuire a riaffermare la natura della RETE come bene pubblico e l’accesso alla conoscenza come diritto fondamentale; 2) favorire il dialogo per identificare l’insieme dei diritti di Internet e, in caso di successo, identificare quali siano le aree e i diritti più rilevanti da prendere in considerazione; 3) iniziare una discussione su come garantire i diritti di Internet.

SESSIONE PLENARIA OPENNESS

Il primo [16] tema del Summit di Atene OPENNESS riguarda la libertà in rete in tutte le sue declinazioni, e in particolare la libertà di raccogliere, elaborare, esprimere e comunicare idee, informazioni, oggetti intellettuali e conoscenze di ogni genere. Questa libertà costituisce l'elemento fondamentale che differenzia Internet, e la Società dell'informazione interconnessa emersa negli ultimi anni dello scorso secolo, dai sistemi di telecomunicazione precedenti e dalle modalità sociali ed economiche che essi esprimevano.

Il moderatore ha aperto la sessione sottolineando che molti dei principi di libertà, riconosciuti sia nella dichiarazione del Summit di Ginevra sia dagli impegni presi a Tunisi, sono stati trascurati e costituiscono ancor oggi una sfida, una minaccia tanto seria da determinare una diminuzione dell'attrazione alla rete. Ha poi citato il caso dell'arresto del blogger greco, e del timore delle istituzioni di alcuni paesi nei confronti di Internet, la loro volontà di controllare la rete, censurarla e sottoporre a pressioni gli utenti creatori di contenuti. L'introduzione ai lavori si è conclusa con un elenco di domande sui diritti umani nella rete e sulla libertà di espressione nella rete, che sono servite a stimolare la discussione da parte del pubblico.

«Quali sono gli esempi di rafforzamento dei diritti umani grazie alla Libertà di espressione?».

«Dovrebbero le maggiori corporates usare il loro potere per modificare i termini secondo i quali si opera in certi paesi?»

«Dovrebbero le corporates rifiutare di conformarsi con leggi non allineate con i diritti umani?

«Dovrebbero gli Internet Service Providers promuovere la libertà di espressione nei paesi ove esistono leggi restrittive?»

«Come si armonizza la pratica del copyright ed i diritti della proprietà intellettuale, con i diritti del consumatore?»

«Quali sono i vincoli accettabili per la Libertà di espressione? Qual'è il quadro delle politiche e regolamentare?»

«Qual'è il dimensionamento della rete compatibile con l' accesso per tutti?»

Steve Ballinger di Amnesty International ha espresso le sue preoccupazioni, non solo nei confronti dei governi con politiche restrittive ma anche nei confronti di quelle corporates che, in aiuto di certi governi, forniscono a loro informazioni che consentono la persecuzione degli utenti. Incoraggiante è il risultato della campagna contro la repressione delle Libertà di espressione in Internet (http://irrepressible.info), che ha avuto un ampio consenso con 50.000 sostenitori da tutto il mondo.

Catherine Trautmann ha parlato della risoluzione del Parlamento Europeo che è stata presa ad unanimità nel Luglio del 2006, invitando il settore privato a tenere presente che gli utenti devono essere protetti ed invitando gli stati a promuovere la libertà di espressione a livello mondiale. Tutti gli attentati alla libertà di espressione devono essere condannati, mentre il settore privato deve cooperare solo con quei governi che rispettano tali diritti.

Anche se sotto la tematica OPENNESS sono compresi molti argomenti, come la libertà dell'infrastruttura della rete, libertà in termini dei diritti civili, ed il ruolo stesso del Forum nel creare una politica internazionale e un quadro di principi, la discussione si è svolta, con toni non sempre pacati, principalmente sui diritti umani, sulla responsabilità sociale dell'impresa e sulla questione della proprietà intellettuale.

SESSIONE PLENARIA SULLA SECURITY

Il tema [17] della SECURITY della rete è potenzialmente molto vasto; questo tema si accompagna spesso ad altri termini quale la robustezza, la ridondanza, la stabilità della rete, etc. Insomma la sicurezza è un tema che tocca la architettura della rete stessa e tutti gli accorgimenti per contrastare gli usi distorti della rete che danneggiano gli utenti e che favoriscono quello che si chiama genericamente "crimine informatico".

La sessione plenaria sulla SECURITY si è svolta senza particolari tensioni, rispetto alla precedente. Molteplici si sono presentati gli argomenti in discussione data la multidisciplinarietà dell'aspetto sicurezza, e data la repentina evoluzione del concetto stesso di sicurezza. Sicurezza intesa sia come protezione fisica della rete sia come protezione dell'utente finale, per cui l'importanza dell'integrità nella trasmissione dei dati, la Privacy e la fiducia nelle operazioni di transazione economica. Sicurezza intesa sia dal punto di vista tecnologico, sia dal punto di vista legislativo, per cui la quantità e qualità della legislazione e il suo impatto nel mondo degli affari. Sicurezza definita secondo i livelli della rete.

La discussione ha toccato il ruolo degli stakeholder e delle istituzioni che operano nel campo della sicurezza richiamando la necessità di una collaborazione più stretta tra le parti. Dato che per ogni cultura il concetto di sicurezza è differente, è emersa la importanza di stabilire una più stretta collaborazione internazionale e di definire le responsabilità delle parti in causa.

Il ruolo e compito dei governi da alcuni è visto solo in funzione della pressione legislativa e politica e come catalizzatore e coordinatore della lotta contro il cyber crime. Dall'altra parte, per altri, vista la sicurezza come un bene pubblico, i governi dovrebbero avere un ruolo attivo nella protezione dell'utente, tramite la fornitura di strumenti gratuiti per la protezione in rete.

Non è passata inosservata la questione relativa alle azioni criminali prodotte dai governi stessi, come anche ci si è domandati sulle modalità secondo le quali dobbiamo relazionarci con quei governi che non consentono le libertà a i loro cittadini.

Non meno critica è la responsabilità degli operatori di rete (ISP e Tier-1 Provider) nel garantire la sicurezza in assenza di politiche pubbliche e standard di sicurezza. Proprio la produzione degli standards è stata criticata, in quanto appare un processo chiuso e pericolosamente gestito da entità molto potenti: per cui si è rimarcata la necessità di promozione di standards aperti e l'utilizzo di strumenti a codice aperto.

Accanto alla protezione dei diritti civili, è necessario fornire una maggiore informazione agli utenti che per la prima volta incontrano Internet. La proposta di un patentino per gli utenti della rete ha stimolato la discussione senza però ricevere grande consenso.

Accennata anche l'importanza dell'assistenza ai paesi in via di sviluppo sulle questioni legate alla sicurezza.

Proposta l'instaurazione di un processo comune ove esperti legali, tecnici e professionisti possano approfondire e coordinare le loro azioni, secondo differenti aree di collaborazione:

1. Quadro legale sugli standards;
2. Modus operandi degli enti certificatori;
3. Livello tecnico;
4. Formazione e costruzione di capacità.

In definitiva quello che è fondamentalmente emerso è la necessità di un rapporto di collaborazione delle parti, e la realizzazione di una task force di coordinamento delle emergenze sulla sicurezza.

SESSIONE PLENARIA DIVERSITY

Il terzo tema DIVERSITY [18] in discussione ad Atene concerne la tutela della diversità culturale come patrimonio comune di tutta l'umanità che in quanto tale va preservata e valorizzata. Lo sviluppo della Società dell'Informazione a livello nazionale ed internazionale deve quindi prevedere, nel rispetto di tale diversità, la produzione di contenuti locali, ovvero in lingua locale e di rilevanza locale.

Il discorso durante questa sessione si è orientato intorno all'importanza della produzione di contenuti locali, per cui il multilinguismo in Rete come elemento fondamentale della promozione della conoscenza, della trasformazione sociale, dello sviluppo umano e della democrazia.

In secondo luogo è stata affrontata la questione dell'internazionalizzazione dei nomi di dominio IDN [19], aspetto molto controverso di carattere linguistico in via di risoluzione. Un esempio significativo della complessità del problema è dato dal Senegal, ove esistono tredici lingue orali che non hanno una propria scrittura, mentre per scrivere si usa o l'alfabeto latino o quello Arabo. La presenza di molte lingue comunemente utilizzate e codificate rende impossibile trovare una soluzione, l'accesso rimane ostacolato anche dall'impossibilità di avere una lingua comune. Un'altro esempio è dato dalla Svezia ove esistono sette lingue ufficiali, di cui sei di queste sono protette dalla legge, l'unica lingua non protetta è lo svedese! il quale risulta protetto in Finlandia.

Come altri, anche Quiheng Hu (Chairman ISOC Cina) ha sostenuto che gli IDN non possono in se costituire una soluzione per la diversità. In Cina esistono dozzine di lingue locali e non è possibile che siano tutte abilitate nel DNS. L'utilizzo di diverse lingue nei nomi di domini potrebbero mettere a rischio la stabilità della rete e comprometterne la sicurezza. Servono politiche intraprese in modo comune, per trovare un compromesso fra multilinguismo dei nomi a dominio, stabilità e sicurezza della rete.

Anche Liz Longworth, rappresentante dell'UNESCO, ha sostenuto che prima di parlare degli IDN, esiste il passo della negoziazione dei caratteri e lingue da codificare. La questione del multilinguismo prescinde i confini nazionali e deve essere affrontato a livello di comunità

linguistiche. Vi è anche una questione di sovranità da risolvere. Gli IDN sono solo identificatori, strumenti che tutti hanno l'interesse di sviluppare, ma non come espressione della propria lingua nativa.

Liz Longworth ha anche precisato il significato del concetto DIVERSITY [20], come strumento per la condivisione della conoscenza, per cui diversità significa l'abilità per gli utenti di partecipare ed esprimere la loro cultura in modo che rifletta la loro identità. La diversità ha a che vedere con la rappresentanza, con quello che noi siamo: donne, giovani, persone con disabilità, indigeni. Come la diversità nella natura, così la diversità nella rete deve riflettere l'intero spettro dell'attività umana, passata e presente. In assenza della diversità non si può parlare di accesso e partecipazione.

Liz Longworth spiega in che modo realizzare un ambiente democratico che garantisca la produzione di contenuti locali da parte degli utenti.

1. La promozione della lingua locale nelle scuole;
2. L'informazione governativa sia a livello locale sia nazionale deve avvenire nelle lingue locali;
3. Centri multimediali per la preservazione della tradizione orale;
4. Facilitatori locali e strumenti convenzionali come la radio;
5. Tradizione orale;
6. Risorse umane in grado di produrre contenuti locali;
7. Politiche a favore di canali comunicativi alternativi;
8. Larghezza di banda.

Per Adama Samassekou (Presidente, dell'Academia Africana delle lingue, Bamako, Mali) i tre pilastri della diversità sono la filosofia, l'etica e la politica. Anzitutto la diversità linguistica costituisce la madre della diversità culturale nella società umana, come in natura è la biodiversità, ossia un modo secondo il quale le specie fondano la sopravvivenza in natura. Diversità per gli africani significa avere la possibilità di condividere la loro conoscenza. Il digital divide non ha tanta importanza quanto la diversità linguistica, fattore determinante per garantire il processo democratico della Internet governance.

Da non dimenticare il problema del valore economico della lingua, e il ruolo di certe autorità e certi governi nell’implementare politiche a favore della diversità linguistica. Come esempio la Francia,

che a causa delle politiche pubbliche dei suoi governi, ha portato il francese ad essere la seconda lingua più diffusa in Internet. Nell'ambito della DIVERSITY il ruolo dei governi diventa di vitale importanza, nell'inclusione di gruppi svantaggiati e di persone diversamente abili.

In discussione l'importanza della conoscenza della lingua inglese da parte degli utenti: in Internet la maggior parte dei contenuti sono scritti in lingua inglese, mentre per certi paesi risulta improponibile dal punto di vista economico spendere per tradurre contenuti dall'inglese alla propria lingua locale. Sono necessari fondi e supporto ai paesi in via di sviluppo, in primo luogo per creare competenze in grado di elaborare sistemi per adattare i contenuti internazionali sulla base delle esigenze locali. Non secondario il problema degli utenti Internet di alcuni stati africani che devono essere messi in grado di produrre autonomamente contenuti nelle loro lingue locali, così come devono avere a disposizione le traduzioni di contenuti internazionali. Segue la necessità dello sviluppo di competenze, e dell'istruzione nelle scuole di linguaggi come C++, Java e Python, e dell'importanza della realizzazione di strumenti efficienti di traduzione automatica.

Raphael Canet (Università di Quebec, Montreal) domanda come garantire la diversità culturale quando non attuabile. Per esempio la UNESCO ha adottato una convenzione sulla protezione della diversità culturale, la quale richiede l'attuazione di politiche pubbliche e di accordi, ma che non tutti i paesi del mondo hanno firmato, come per esempio Israele e Stati Uniti. In pratica, Canet sostiene che abbiamo due filoni, uno politico che vede la diversità come un bene comune, ed uno economico che dipende dalla sostenibilità.

In discussione gli alti costi per l'utilizzo dei contenuti e il ruolo fondamentale che possono svolgere gli standards aperti e il software libero. Grazie al software libero in Colombia vi sono stati sviluppi positivi, nell'ambito delle popolazioni indigene, sullo scambio delle informazioni e la tutela di tali informazioni che riguardano la loro eredità culturale. In definitiva in molti hanno concordato che soluzioni offerte dal software libero possono facilitare la produzione e la disseminazione di contenuti. In causa anche la trasparenza operativa dei sistemi di ricerca.

Vint Cerf - Chair del Board di ICANN - ha parlato dell'importanza della produzione di contenuti orali. A proposito è stato citato come esempio l'India, ove hanno realizzato centri informativi audio visuali che non si limitano all'installazione di computer ma offrono servizi ed informazioni.

SESSIONE PLENARIA ACCESS

La connettività [21] è un elemento abilitante indispensabile: senza la possibilità di interagire attraverso strumenti informatici all'interno di una comunità mondiale, ha un senso limitato parlare di Società dell'Informazione e tanto meno di Internet Governance.

La sessione su ACCESS è iniziata sottolineando che solo un sesto della popolazione mondiale è collegata in Internet, solo il 40% degli Asiatici può usufruire di banda larga e in Africa questa percentuale scende al 0.1% della popolazione. Comunque complessivamente il dato sul divario del digital divide si è ridotto di 20 punti (da 27 a 7) nel periodo tra il 1994 e il 2004.

Il problema dell'accesso non riguarda esclusivamente l'accesso alle tecnologie ma viene inteso anche come accesso ai contenuti, ai servizi, alla conoscenza, alla formazione ed anche alla certificazione.

La sessione ha dato particolare attenzione al continente africano ove il problema primario rimane la fame, l'analfabetismo, la povertà e il sottosviluppo. Determinante per il loro sviluppo è la loro partecipazione nella comunità scientifica mondiale, almeno garantendo loro l'accesso a bassi costi alle pubblicazioni scientifiche. La formazione rimane una delle barriere più imponenti per l'accesso; alcuni hanno sostenuto che il software libero e gli standards aperti possono avere un ruolo determinante. Sottolineata anche la problematica dei brevetti software, i quali creano monopoli compromettendo così l'interoperabilità. Sulla questione dei brevetti software non sono stati tutti d'accordo, alcuni hanno affermato che i brevetti non costituiscono in se un problema, ma che comunque il loro utilizzo deve essere indirizzato in tal modo, da non compromettere la possibilità di implementare le tecnologie ricoperte dai brevetti stessi.

La barriera primaria dell'accesso in rete rimane il costo di connessione, problema che non riguarda esclusivamente i paesi in via di sviluppo. Per esempio il costo di connessione tra l'Inghilterra e New York si aggira sui 120 mila Euro per una velocità di 10 Gbit/s, invece il costo per collegare Atene con Instabul è intorno ai 2 milioni di Euro per una velocità di 620 Mbit/s.

Un'altro esempio citato, l'Argentina, ove il costo di connessione in Internet, tramite il cavo sottomarino, si aggira sui 15-20.000 $ per una velocità di 155Mbit/s. Per cui approssimativamente, a parità di costo i paesi sviluppati usufruiscono di velocità sostanzialmente superiori. Per aggirare questo problema, in Sud America sin dal 1998, si stanno realizzando exchange points locali tra l'Argentina, il Brasile ed altri paesi della regione, così il traffico locale viene veicolato

regionalmente senza dover passare dal backbone internazionale o dover pagare il transito agli Stati Uniti. A proposito è stata proposta la realizzazione di una infrastruttura regionale Africana, in quanto solo così sarà possibile la riduzione dei prezzi, come è avvenuto in Europa ove gli operatori delle telecom hanno costruito una rete in comune, la quale ha consentito la riduzione dei costi. Un esempio della gravità della situazione è dato dal Burkina-Faso, che ha la connessione in Internet tramite il Senegal ed è costretta a pagare sia per l'accesso, sia per il servizio ed il transito.

Per alcuni la questione più importante inerente l'accesso, riguarda il problema del monopolio del local loop, per cui diventa fondamentale identificare le barriere alla competitività e la modalità per sormontarle. Per tale fine diventa necessaria una regolamentazione trasparente in grado di stimolare la competitività per favorire l'accesso. Dall'altra parte è stato messo in evidenza anche l'importanza dell'aspetto collaborativo, nella risoluzione dei problemi che riguardano specialmente i gruppi svantaggiati. È una questione di costi; il servizio deve essere considerato come un bene pubblico prioritario, come se fosse cibo o abitazione, ha affermato Kishis Park (Presidente del IPv6 Forum). Per altri la soluzione per l'accesso in Africa deve essere intrapresa a livello nazionale, con realizzazione di soluzioni innovative e a basso costo.

È infine stata sottolineata l'importanza della mobilizzazione di capitali a livello locale, e l'apertura dei mercati svincolati dalla giurisdizione dei governi. Alcuni altri hanno sostenuto che i governi non possono rimanere estranei alla questione, in quanto i servizi pubblici come la sanità, la formazione e le banche implicano un maggiore ruolo del settore pubblico. Per esempio nelle aree rurali economicamente svantaggiate tra Brasile e Colombia, ove il settore privato non ha interessi, gli access points sono stati finanziati dai rispettivi governi.

Le tecnologie wireless potrebbero cambiare drasticamente lo scenario, in quanto facilitano la costruzione di local loop e sono più semplici da usarsi anche da parte di persone che non hanno grandi conoscenze tecniche. In discussione anche la telefonia mobile come soluzione per l’accesso. C’è chi è a favore e chi sostiene che non si può estrapolare il modello della telefonia mobile in relazione con Internet, in Europa e negli Stati Uniti non si identifica la Società dell'informazione con la diffusione della telefonia mobile, ma si parla di Società dell'Informazione grazie a l'avvento delle rete Internet e dei servizi che essa può offrire.

La sessione si è conclusa ribadendo che i tre pilastri fondamentali per la Rete Internet, già definiti dalla Commissione Europea, sono: la Libertà, Interoperabilità e Neutralità.

SESSIONE PLENARIA THE WAY FORWARD

La sessione è iniziata con un breve riassunto dei lavori delle sessioni precedenti, e in seguito sono stati effettuati degli annunci su iniziative, alcune delle quali intraprese durante il Forum. Significativa l'iniziativa GIGANet [22] (Global Internet Governance Academic Network), una comunità internazionale di ricerca accademica sulla Internet Governance. Una partnerhip nata ed annunciata proprio nell'ambito dell'IGF. In seguito la sessione ha sottolineato l'importanza di trovare soluzioni a favore dei paesi in via di sviluppo, ed agevolare la loro partecipazione nell'ambito dell'IGF. Sottolineata l'importanza del dialogo multi stakeholder intrapreso, discusso il ruolo del Forum e una probabile agenda del forum di Rio, con l'inclusione di tematiche come la violenza contro le donne e la pornografia. In discussione il modus operandi delle coalizioni dinamiche, interessante anche la proposta di una coalizione dinamica, con la finalità di aiutare con finanziamenti i paesi in via di sviluppo, ed incrementare così la loro partecipazione all'IGF.

SESSIONE PLENARIA EMERGING ISSUES

La sessione è stata dedicata per lo più ai giovani, all'importanza di investire su di essi e di coinvolgerli in questo processo. Sottolineata la necessità della realizzazione di corsi Universitari sulla Internet Governance. In discussione il ruolo dell'IGF nella promozione di un ambiente sicuro per i giovani, e la contrapposizione delicata tra libertà e controllo. In discussione il significato del concetto dell'accesso per i giovani, e la disparità dell'accesso in rete tra uomini e donne nei paesi in via di sviluppo. Sottolineata l'importanza di una relazione simbiotica tra i giovani e il mondo degli affari, e il ruolo che la rete Internet può avere nel promuovere la partecipazione al processo democratico, auspicando che l'accesso universale alla rete diventi un diritto umanitario basilare per le future generazioni.

NOTA CONCLUSIVA

In definitiva, l'auspicio dell'Ambasciatore Nitin Desai, che il Forum diventasse un luogo d'innovazione e di "brainstorming", si è verificato con successo, fino al punto che l'IGF ha inaugurato una nuova era di dialogo Universale che rimarrà nodo principale nella storia dell'umanità.

NOTE

[1] IGF vedi: http://www.intgovforum.org/, IGF di Rio vedi: http://www.igfbrazil2007.br/

[2] http://www.wsis.org

[3] vedi Documento Tunis Agenda for the Information Society: WSIS-05/TUNIS/DOC/6 Second Phase of the WSIS (16-18 November 2005, Tunis)

[4] Agenda di Tunisi per la Società dell'Informazione, art.73: "The Internet Governance Forum, in its working and function, will be multilateral, multi-stakeholder, democratic and transparent. To that end, the proposed IGF could build on the existing structures of Internet Governance, with special emphasis on the complementarity between all stakeholders involved in this process – governments, business entities, civil society and inter-governmental organisations;"

[5] vedi documento WSIS-II/PC-3/DOC/05 PrepCom-3 (Geneva, 19-30 September 2005) Report from the Working Group on Internet Governance

[6] Vedi Agenda di Tunisi per la Società dell'Informazione, art.72

[7] La definizione di Internet Governance è stata stabilita durante il controverso processo WSIS: "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 principi, norme, regole, procedure decisionali e programmi condivisi che determinano l'evoluzione e l'uso di Internet."

[8] Agenda di Tunisi per la Società dell'Informazione, art.77:"The IGF would have no oversight function and would not replace existing arrangements, mechanisms, institutions or organizations, but would involve them and take advantage of their expertise. It would be constituted as a neutral, non-duplicative and non-binding process. It would have no involvement in day-to-day or technical operations of the Internet".

[9] IGF di Atene vedi: http://www.intgovforum.org/meeting.htm)

[10] « ... Il Governo guarda con attenzione al tema delle regole della rete: durante lo scorso Internet Governance Forum di Atene, è stata proprio l'Italia a proporre la redazione di una Carta dei diritti e dei doveri di Internet» - ha così commentato il Sottosegretario Beatrice Magnolfi, al termine dei lavori di Atene «Nella rete di seconda generazione - ha aggiunto - in cui i contenuti sono prodotti

dagli utenti, con livelli bassi o inesistenti di intermediazione, insieme alla libertà di esprimere il proprio pensiero, deve crescere anche la responsabilità personale delle azioni che si compiono....»

[11] vedi il comunicato del ministro Nicolais http://www.innovazionepa.it/ministro/salastampa/comunicati/131.htm

[12] I risultati della consultazione virtuale sono disponibili a http://listserv.iit.cnr.it/internetgovernance.html, lo spazio nato allo scopo di assicurare a tutti i cittadini interessati all'IGF la possibilità di contribuire al dibattito pubblico sulle grandi tematiche in discussione ad Atene. La consultazione si è svolta dal 1 al 22 ottobre 2006. I contributori hanno inviato messaggi via posta elettronica.

[13] Leggi il discorso di Vint Cerf che ha tenuto durante la sessione inaugurale dell'IGF di Atene:

http://www.icann.org/announcements/announcement-italian-1-30oct06.htm

[14] vedi comunicato sul sito del Ministro per le Riforme e le Innovazioni nella P.A. http://www.innovazionepa.it/ministro/salastampa/comunicati/244.htm

[15] http://www.liberosapere.org/fks/no1984/costituzione-rete.html

[16] dal documento del Comitato consultivo sulla governance di Internet preparato da Vittorio Bertola e Fiorello Cortiana su OPENNESS disponibile a http://www.isoc.it/index.php?option=com_content&task=view&id=218&Itemid=21

[17] dal documento del Comitato consultivo sulla governance di Internet preparato da Laura Abba, Antonino Mazzeo e Stefano Trumpy sulla SECURITY disponibile a http://www.isoc.it/index.php?option=com_content&task=view&id=221&Itemid=21

[18] dal documento del Comitato consultivo sulla governance di Internet preparato da Matilde Ferraro e Vittorio Bertola e Fiorello Cortiana sulla DIVESRITY disponibile a http://www.isoc.it/index.php?option=com_content&task=view&id=219&Itemid=21

[19] Sulla questione degli IDN leggi:

Internationalising Top Level Domain Names: Another Look (ISOC)
http://intgovforum.org/Substantive_1st_IGF/briefing18.pdf
[20] Documenti relativi:

The universal declaration on cultural diversity
http://unesdoc.unesco.org/images/0012/001271/127160m.pdf

Recommendation on multilingualism and universal access

http://portal.unesco.org/ci/en/ev.php-URL_ID=13475&URL_DO=DO_TOPIC&URL_SECTION=201.html

[21] dal documento del Comitato consultivo sulla governance di Internet prodotto da Joy Marino e Laura Abba dedicato al tema ACCESS disponibile a http://www.isoc.it/index.php?option=com_content&task=view&id=220&Itemid=21

[22] http://www.igloo.org/giganet