Garante per la protezione dei dati personali

INTERNET E PRIVACY: QUALI REGOLE?

ATTI DEL CONVEGNO

SUPPLEMENTO N. 1
AL BOLLETTINO N. 5

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
DIPARTIMENTO PER L'INFORMAZIONE E L'EDITORIA

INDICE

I GIORNATA - VENERDÌ 8 MAGGIO 1998

On. Prof. Stefano Rodotà

Presidente, Garante per la protezione dei dati personali

Signor Vice-Presidente del Consiglio, Autorità, Signore e Signori, il caso o una qualche astuzia della storia, propiziate però dalla collaborazione del Ministro dei Beni Culturali che qui pubblicamente voglio ringraziare, hanno fatto sì che questo nostro incontro sul problema oggi più acuto dell'innovazione tecnologica si svolgesse in questo salone che sicuramente per il grande affresco di Pietro da Cortona è uno dei luoghi più alti del barocco romano. E' una coincidenza e nulla di più che io vi voglio segnalare. Del barocco si è detto: che potenziò in sommo grado tutte le possibilità tecniche ed espressive dell'artista, lo abituò a corrispondere alle più svariate esigenze servendosi delle più svariate materie, dal marmo prezioso allo stucco, dal legno al metallo. Cancellò ogni limite alla possibilità rappresentativa dell'arte, introdusse forme e contenuti nuovi.

Oggi e domani dobbiamo proprio discutere di limiti ormai superati, di contenuti nuovi, di inedite possibilità rappresentative. Internet è tutto questo. E quindi consideriamo come un singolare auspicio la congiunzione in questa sala tra antico e futuro.

Discutiamo in Italia ma abbiamo voluto, fin dall'inizio, riconoscere l'impossibilità di chiudersi nella dimensione nazionale e perciò abbiamo chiamato a dare il loro contributo alcuni dei massimi esperti mondiali in questo campo. Sappiamo che è in corso un grande confronto tra Europa e Stati Uniti e perciò siamo assai grati all'amministrazione americana per aver voluto essere ufficialmente presente. Siamo in Europa ed è quindi di grande significato la presenza cospicua di esperti dell'Unione Europea, e in particolare è importantissimo l'intervento che avremo dei commissari Emma Bonino e Mario Monti. Abbiamo avvertito la necessità di un dialogo istituzionale impegnativo che il governo ha condiviso, come testimonia la presenza che qui avremo dei Ministri della giustizia e delle comunicazioni e in primo luogo del Vice-Presidente del Consiglio Valter Veltroni che di nuovo ringrazio molto e al quale ho il grande piacere di dare la parola.

APERTURA DEI LAVORI

On.Valter Veltroni
Vice-Presidente del Consiglio dei Ministri

I progressi compiuti dalle tecnologie dell'informazione e della comunicazione stanno rapidamente cambiando il nostro stile di vita e di lavoro, i modelli tradizionali di educazione, di studio e di ricerca. Effetti profondi sono già visibili e si manifesteranno in futuro con sempre maggiore evidenza in tutti gli aspetti della nostra vita quotidiana: sui processi di produzione e sui prodotti, sulle reti di distribuzione e nelle relazioni sociali, toccando settori che qualche decennio fa apparivano come entità separate.

Questa nuova sfida tecnologica, come tutte le grandi rivoluzioni, provoca paura, ansia, preoccupazione ma, al tempo stesso, favorisce la creazione di nuove risorse e genera nuove opportunità. Opportunità di diffusione della conoscenza; opportunità di scambio e di arricchimento reciproco; opportunità di crescita della democrazia. Le nuove tecnologie, e fra queste Internet, avvicinano i popoli e le culture, ne facilitano la conoscenza reciproca; riducono le distanze.

Le nuove tecnologie ci offrono grandi promesse e un notevole carico di speranze. Ma ci espongono anche a grandi rischi: appiattimento culturale, perdita delle diversità culturale, nuove diseguaglianze.

Tutto il mondo è di fronte a questa sfida. Ma una posizione del tutto particolare è quella dell'Europa. Il processo di integrazione europea, che solo pochi giorni fa ha segnato una tappa fondamentale con il battesimo a Bruxelles della moneta unica, non deve avvenire con la perdita di uno dei più importanti valori delle nazioni europee: la specificità delle singole culture. Nel nostro continente, allora, le opportunità, ma anche i rischi collegati alla diffusione delle nuove tecnologie dell'informazione, si presentano moltiplicati. E non è un caso che le istituzioni comunitarie abbiano da tempo dedicato molto spazio di riflessione e di iniziativa regolamentare in questo settore.

Mai come oggi è vera l'affermazione di Francis Bacon: "il sapere è in sé stesso potere". L'era digitale può diventare un'epoca di nuove, profonde diseguaglianze: non solo fra le diverse nazioni e aree del mondo, ma anche all'interno di ciascun paese. Diseguaglianze di tipo nuovo, legate all'accesso alla conoscenza e ai nuovi strumenti della conoscenza. Temo che il millennio che abbiamo di fronte potrà segnare conflitti sociali di tipo nuovo, aspri quanto quelli che sono stati determinati dalla rivoluzione industriale. Se poche persone avranno il possesso della conoscenza e degli strumenti della comunicazione, avremo decretato nuove gerarchie, nuove forme di esclusione sociale.

In ragione dei pericoli di queste nuove disuguaglianze, dovremo combattere l'analfa-

betismo tecnologico così come in passato abbiamo combattuto l'analfabetismo delle lettere.

Dovremo avviare programmi di investimento a sostegno del capitale umano, attraverso l'istruzione di base e la formazione continua degli adulti. Trasformare le infrastrutture culturali esistenti in luoghi di alfabetizzazione informatica. Penso alla creazione di accessi pubblici alle reti nelle biblioteche, nei musei, nelle scuole, nelle università, tutte istituzioni che potranno entrare pienamente a far parte della rivoluzione tecnologica e diventare un eccezionale veicolo per la sua diffusione.

Per realizzare questo programma, abbiamo bisogno di dare vita a nuove politiche.

Credo che si debba cominciare a guardare ai problemi di accessibilità alla cultura come a un pezzo del nuovo sistema di welfare che dobbiamo costruire. Un sistema votato ai diritti di cittadinanza e all'uguaglianza di opportunità, calibrato sui bisogni attuali della nostra società, sulle sue esigenze di crescita e di riduzione delle distanze sociali.

Il nostro governo ha accolto la sfida lanciata dalle nuove tecnologie dando priorità all'istruzione e alla formazione, ben sapendo quanto il cattivo funzionamento delle nostre istituzioni formative conti per spiegare l'analfabetismo informatico di una parte ancora troppo grande degli italiani. Vorrei citare per tutti il Programma Mediateche, nell'ambito del quale è stata già finanziata ed è in fase di realizzazione la costruzione di una mediateca nella ex chiesa di Santa Teresa a Milano, con trecento accessi ad Internet presto disponibili al pubblico e collegati con i giacimenti librari della Biblioteca Braidense.

Sono convinto che le nuove tecnologie rappresentino realmente una grande opportunità per migliorare la qualità della vita, ma vedo anche grandi rischi. Un rischio, se vogliamo definirlo così, economico pur se strettamente legato alla sfera della creatività: il diritto d'autore. La riproducibilità delle opere mette in crisi il diritto d'autore, tradizionale meccanismo di sostegno finanziario della produzione culturale. Bisogna quindi creare e affinare strumenti che siano in grado di proteggere la fantasia e il lavoro anche nella "grande ragnatela" senza impoverire i contenuti che attraverso di essa possono arrivare a milioni di persone. Un primo passo potrebbe essere la specializzazione dell'offerta: segmentare la rete attuale in reti specializzate permetterebbe di indirizzare l'offerta culturale e di creare luoghi di autentico scambio e confronto, tutelando al tempo stesso gli autori. In questo quadro, credo che allo Stato spetti il compito di assicurare a tutti la possibilità di produrre, mettere in circolo e insieme tutelare idee, saperi, conoscenza. Saranno il mercato, le società private, l'iniziativa dei singoli a mettere insieme offerta e domanda di sapere in rete.

Se contro il rischio di obsolescenza del diritto d'autore dobbiamo intensificare gli sforzi nella ricerca tecnologica, il pericolo dell'appiattimento culturale, di nuove forme di "monoculturalismo", si supera con la specializzazione dell'offerta e con la sua moltiplicazione negli innumerevoli segmenti in cui si presenta la domanda effettiva o potenziale di sapere e di conoscenza. Il futuro è nelle reti ad alto grado di specializzazione, ad elevata qualità, in grado di innovare e selezionare l'offerta per la domanda che intendono soddisfare. A decidere deve essere il mercato. Lo Stato si deve preoccupare soltanto di creare le condizioni per fare in modo che a produrre siano in tanti, che ci siano tanti soggetti che mettono in circolo tante idee diverse.

Vi è un solo settore con riferimento alle nuove tecnologie in cui l'intervento diretto dello Stato è legittimo e necessario: è quello della tutela della privacy. Contro il pericolo che il massimo della libertà concessa da questi strumenti coincida con il minimo di autonomia e di garanzia individuale, il Parlamento ha approvato una legge che, recependo i principi ispiratori della Direttiva europea dell'Ottobre 1995, ha posto il nostro Paese all'avanguardia in Europa. L'intensa attività del Garante in questo primo anno di applicazione della legge dimostra che in Italia si sta diffondendo una nuova sensibilità, una "cultura della privacy" che rappresenta il migliore antidoto che la società civile può esprimere contro il rischio di un Grande Fratello tecnologico. In questo settore va cercato, come ha detto bene Stefano Rodotà, un delicato equilibrio tra "vuoti" e "pieni" di diritto. Bisogna guardare e scegliere con attenzione tra quanto è legittimo e quanto è arbitrario da parte dello Stato.

Delimitare quel delicato confine che esiste tra la libertà di comunicare e forme di comunicazione invasive della sfera privata dei singoli. Lo Stato deve abdicare ai propri doveri di controllo in nome della libertà di informazione e di espressione? Credo di no.

Credo anzi che tutti gli Stati, insieme, abbiano il dovere di intervenire istituendo regimi di tutela rispettosi delle diverse specificità culturali, ma anche il dovere di compiere un lavoro comune di armonizzazione delle legislazioni.

In questa sede merita di essere richiamato un altro problema, più specificatamente legato alla diffusione e all'utilizzo di Internet: il problema della tutela dei minori. Non è possibile trascurare i rischi legati a questo nuovo, incredibile scenario nel quale si mescolano in modo indifferenziato suoni e immagini tratti da cartoni animati per bambini e da riviste per adulti, senza alcuna differenza nella modalità di accesso. In America sono stati elaborati sistemi di selezione e di filtraggio dei contenuti di violenza criminale, sessuale o verbale. Si tratta di software che si trovano in commercio in Europa e anche in Italia.

Ma dare una soluzione tecnologica al problema può non essere sufficiente. In questo modo infatti si corre il rischio di deresponsabilizzare i produttori e i distributori di contenuti, demandando i compiti di tutela alle sole famiglie, e si rischia di sottrarre visibilità istituzionale al problema, che esige invece una qualche forma di regolamentazione normativa. E' attualmente in corso di discussione al Senato la normativa contro lo sfruttamento sessuale dei minori che, recependo i principi contenuti nella Convenzione sui Diritti dell'Infanzia di New York, stabilisce pene severe per chi produce, diffonde e mette in commercio con qualsiasi mezzo materiale pornografico concernente minori. Si tratta di un primo passo, ma bisogna anche intervenire con una costante opera di sensibilizzazione degli adulti e formando le capacità critiche dei bambini, attraverso l'educazione e l'alfabetizzazione informatica.

In conclusione, di fronte alle sfide che le nuove tecnologie impongono, il compito dei Governi si riassume in un triplice obiettivo: garantire e 'democratizzare' l'accesso alla cultura e alle reti, che in tanta parte del mondo è ancora negato da vincoli economico-sociali e da carenze infrastrutturali; garantire lo sviluppo concorrenziale dei nuovi mercati che si creano attraverso la progressiva convergenza di telecomunicazioni, informatica e audiovisivo, perché la libertà di accesso a questi mercati è garanzia fondamentale di democrazia; e,

infine, creare le condizioni perché cresca liberamente la capacità di produzione di contenuti sulle nuove reti, per permettere che l'informazione si trasformi in conoscenza.

Se sapremo governarla con intelligenza, la società dell'informazione non porterà alla desertificazione e all'impoverimento culturale, ma al contrario sarà la condizione per una nuova stagione di produzione culturale. L'innovazione dei linguaggi sarà la chiave per tutti i settori della cultura, dalla letteratura al teatro, dalle arti visive al cinema. Le culture locali non verranno inghiottite, ma si moltiplicheranno le occasioni di contatto e di nuove contaminazioni. Se sapremo cogliere e governare questa grande occasione di cambiamento, le generazioni future non vedranno avverarsi la sinistra profezia orwelliana, con un nuovo, tetro ordine imposto dalla tecnologia avanzata, ma vedranno avverarsi le condizioni per esprimere nuove fantasie ed emozioni, in un nuovo disordine creativo.

Prof. Stefano Rodotà

Ringrazio molto il Vice-Presidente del Consiglio, sappiamo tutti quali siano i tempi e i ritmi dell'attività di governo e quindi un ringraziamento particolare per essere stato qui in questa mattinata e buon lavoro.

I SESSIONE

Prof. Giuseppe Santaniello
Vice-Presidente, Garante per la protezione dei dati personali

Diamo inizio ai lavori della prima sessione. Prima di tutto devo comunicare che il Sindaco Rutelli, impegnato per ragioni d'ufficio fuori Roma, manda il suo fervido saluto a tutti i partecipanti al convegno.

Il tema della prima sessione è uno dei punti centrali di tutto il sistema di tutela della riservatezza e della identità personale. Potremmo dire che è uno dei tratti maggiormente qualificanti della problematica e introduce e realizza una tutela talmente ampia e talmente innovativa della quale già il Presidente Veltroni ha tracciato i momenti fondamentali e i momenti innovativi.

Relatore è il Presidente del Garante per la protezione dei dati personali, on. Prof. Rodotà.

RELAZIONE INTRODUTTIVA

Prof. Giuseppe Santaniello
Vice-Presidente, Garante per la protezione dei dati personali

Diamo inizio ai lavori della prima sessione. Prima di tutto devo comunicare che il Sindaco Rutelli, impegnato per ragioni d'ufficio fuori Roma, manda il suo fervido saluto a tutti i partecipanti al convegno.

Il tema della prima sessione è uno dei punti centrali di tutto il sistema di tutela della riservatezza e della identità personale. Potremmo dire che è uno dei tratti maggiormente qualificanti della problematica e introduce e realizza una tutela talmente ampia e talmente innovativa della quale già il Presidente Veltroni ha tracciato i momenti fondamentali e i momenti innovativi.

Relatore è il Presidente del Garante per la protezione dei dati personali, on.Prof. Rodotà.

RELAZIONE INTRODUTTIVA

LIBERTÀ, OPPORTUNITÀ, DEMOCRAZIA E INFORMAZIONE

On. Prof. Stefano Rodotà

Non è facile giungere al cuore di Internet e coglierne la realtà vera, bisogna liberarsi con pazienza di molta retorica, superare diffidenze, evitare trappole ideologiche, non restare abbagliati da quella che è stata chiamata la *Internet Trinity*, una trinità fatta dalla tecnologia del mezzo, dalla distribuzione geografica dei suoi utenti, dalla natura dei suoi contenuti.

Le discussioni si sono venute intensificando, soprattutto nel corso dell'ultimo anno, ma in esse si possono ritrovare tomi e temi che abbiamo già conosciuto all'inizio dei dibattiti intorno alla introduzione dei computer nella nostra organizzazione sociale.

Nel 1965 un osservatore tutt'altro che sprovveduto, come Paul Baran, scriveva in un rapporto per la Rand Corporation (cito): "non aspettiamoci che il contributo dei giuristi possa sostituire una buona progettazione tecnica, anche se non si volesse tenere conto del ritardo sociale dei procedimenti legislativi e giudiziari, gli specifici problemi del mondo dei computer si collocano in una dimensione che ad essi, ai giuristi, sfugge completamente".

Non voglio dire che questa superbia tecnologica, questo orgoglio tecnologico è stato smentito dal fatto che negli anni successivi, nei trenta e più anni che abbiamo alle spalle, si sono venute accumulando moltissime leggi. Ormai, la legislazione sulla *privacy* e sui settori a questa connessi riempie una consistente biblioteca e attraverso questo intenso intervento legislativo si è anche venuta ridefinendo, vorrei dire rivoluzionando la nozione stessa di *privacy*.

Oggi il problema si ripropone; da molte parti si afferma la capacità autoregolativa della nuova tecnologia che si manifesta in rete, delle molte tecnologie che si congiungono dando origine alla rete. E si prospetta una sorta di invincibile contrasto tra le potenzialità tecnologiche e i rischi dell'intervento legislativo, quasi che si trattasse di mondi non comunicanti.

Se usciamo da questa contrapposizione di maniera e guardiamo i fatti, ci possiamo accorgere che proprio nel Paese, gli Stati Uniti, dove più marcata è la diffidenza verso l'intervento legislativo, nel giro dell'ultimo anno si sono venute moltiplicando le iniziative di tipo legislativo. Mi limito a ricordare che, alla fine del '97, erano stati presentati al Congresso degli Stati Uniti sei *bills*, sei proposte di legge sulla *on-line privacy*, due sul trattamento fiscale delle transazioni su Internet, tre sulla crittografia, due sulla proprietà intellettuale e altri progetti si sono venuti aggiungendo in questi mesi, ma è particolarmente significativo il fatto che in tutti e 50 gli Stati americani siano state prese iniziative, alcune delle quali già arrivate alla conclusione dell'approvazione di una legge nelle materie specifiche del

commercio elettronico e della firma digitale.

Quindi ci troviamo di fronte all'avvio di una attività legislativa assai più intensa di quello che aveva segnato l'esordio delle tecnologie elettroniche della comunicazione.

Possiamo aggiungere - ma non voglio insistere in questa carrellata in giro per il mondo - che molte ormai sono nei diversi emisferi del mondo, le iniziative e le leggi che già affrontano questioni specifiche legate all'uso di Internet e regole anche particolarmente penetranti, come quelle che riguardano la trasmissione di "messaggi spazzatura", i *junk E-mail*, che ha costituito oggetto da anni di interventi negli Stati Uniti, di interventi in Europa (in Germania una decisione giudiziaria, in Italia in un decreto di prossima pubblicazione), il divieto dell'invio per ragioni commerciali, senza il precedente consenso dell'interessato, di qualsiasi messaggio con telefonate automatizzate, fax o posta elettronica.

Dunque, la dimensione istituzionale, la dimensione giuridica è tutt'altro che estranea già in questa fase iniziale, formativa, alla questione di quali regole per Internet.

Ma se noi torniamo di nuovo alle discussioni degli anni settanta, troviamo un altro motivo ricorrente. Allora erano consueti, abituali nella discussione libri e scritti che avevano nel titolo la formula, l'espressione "la morte della privacy". Tornano di nuovo, con riferimento a Internet, con riferimento al servizio on-line, le formule "la morte della privacy".

Il rischio esiste, ma forse c'è da tenere conto del fatto che così come nella prima fase di decollo di queste nuove tecnologie, la *privacy* è uscita fortemente trasformata e per molti versi rafforzata, così oggi si offre una ulteriore opportunità di riflessione su questo tema.

Terzo ritorno di temi del passato: faccio qui un riferimento alla situazione italiana.

Molti dei presenti ricordano che, a metà degli anni sessanta e nella prima parte degli anni settanta, la liberalizzazione nel settore delle televisioni e delle radio, fece nascere una generosa illusione di una libertà conquistata per cui sarebbe stato possibile a tutti ampliare le possibilità di comunicazione e di dialogo proprio attraverso televisioni libere, radio libere e per questo si affermava che questa libertà sarebbe stata tanto maggiore quanto minore fosse stata invece la regolazione pubblica.

Noi conosciamo in Italia l'esito di questa vicenda; questa illusione generosa si è spenta in breve tempo, proprio l'assenza di un quadro di regole istituzionali ha favorito il prevalere di pure logiche di mercato. Le televisioni libere sono diventate oggetto di attenzione dei grandi gruppi e questa illusione di libertà è stata riassorbita nelle grandi strutture di tipo oligopolistico. I *digital libertarians*, coloro i quali affermano che la rete è il luogo di una infinita libertà, che non deve essere in alcun modo limitata perché altrimenti correrebbe il rischio di essere compressa e negata, dovrebbero forse tenere d'occhio queste esperienze del passato: la libertà ha sempre bisogno di un quadro istituzionale non che la protegga, ma che consenta ad essa di rimanere al riparo dai molti attacchi che alla libertà possono essere portati anche senza una volontà censoria. E nel momento in cui Internet evolve come grande luogo di interessi economici, tendenza che non può e sarebbe sbagliato contrastare, dobbiamo però tenere conto della necessità di salvaguardare in rete i diritti e le dinamiche della libertà. Non è un caso che da anni si parli e si invochi un *information bill of rights*, che si parli di una "*carta di diritti dell'informazione*" che poi concretamente, almeno nel quadro e

nello spazio dell'Unione Europea, comincia a tradursi in atti significativi e certamente alla fine di quest'anno si avrà una novità senza precedenti: la creazione di uno spazio giuridico europeo dove la tutela della *privacy* e tramite essa la tutela di libertà fondamentali dei cittadini avrà probabilmente il grado più intenso che si conosca al mondo.

Comunque, nell'ultimo anno la discussione si è arricchita, si è fatta più riflessiva, meno unilaterale, mettendo a fuoco i molteplici problemi e le diverse potenzialità di Internet. Che si comincia a percepire sempre più nettamente non come una dimensione separata, così come era avvenuto troppe volte in passato; non come uno spazio del tutto autonomo, del quale i suoi primi frequentatori vorrebbero rimanere gli unici abitanti, ma Internet si manifesta sempre più nettamente come un potente strumento di trasformazione della società.

Di fronte a noi abbiamo davvero un modello di organizzazione sociale. In due sensi: nel senso proprio, perché si propone alla società un suo modo di organizzarsi. Non più l'organizzazione piramidale, ma l'organizzazione a rete. Non più un'organizzazione con una comunicazione a suo modo autoritaria, dall'alto verso il basso, e anche le prime forme di interattività non modificavano radicalmente questo schema, ma davvero come una possibilità di una rete di rapporti che consenta a ciascuno di entrare in rapporto con gli altri mettendo in discussione l'assetto gerarchico dell'organizzazione sociale.

Non ci sono privilegi nel comunicare, anche la più ricca delle strutture di tipo tradizionale, la televisione dei 500 canali, non ha le potenzialità di rottura dello schema gerarchico che abbiamo conosciuto, perché non tutti possono nello stesso tempo assumere il ruolo di produttori e consumatori delle informazioni.

Quante volte in questi anni abbiamo assistito alla rottura da parte di singoli utenti della rete di schemi di controllo sociale, ad esempio mettendo in rete informazioni sgradite ai governi, sgradite ai gruppi economici che sui tradizionali mezzi di informazione non avevano trovato assolutamente alcuna eco.

Questo è un modello di organizzazione sociale, che tuttavia deve essere valutato anche con spirito critico. Ma Internet è un modello di organizzazione anche per quanto riguarda se stessa. Internet non è immobile: ha generato Intranet, ha generato cioè delle reti a loro modo chiuse ma tuttavia anche di grandi dimensioni, e in prospettiva questa è una dinamica da tenere presente. Internet genera la Internet II, la *next generation Internet*, di cui ha parlato nel suo discorso Clinton, la rete superveloce. Un luogo di ulteriori privilegi o un luogo che consentirà la migliore utilizzazione delle potenzialità di questo insieme di nuovi mezzi? Questo è un problema che abbiamo di fronte.

Quindi, in un doppio significato, Internet si presenta come modello sociale.

Ma Internet si diffonde non solo negli spazi sociali, ma per così dire occupa lo spazio della mente. Impone un altro modo di essere, di pensare, di percepire se stessi in rete.

Quante volte, inverando una profezia di William Gibson in Neuromant, abbiamo letto nelle ultime settimane di persone che si sono trovate ad avere una sorta di problema di personalità per essere state private della possibilità di rimanere in rete.

Internet dunque non è solo un modello, lo sappiamo tutti, è anche uno spazio. È uno spazio sociale, uno spazio politico, uno spazio economico, uno spazio altamente simbolico,

che permette nuove forme di rappresentazione del sé, incide sulle identità, consente nuove forme di espressione e di esperienza artistica. Non sono spazi separati. Non si può pensare Internet sezionandola. La globalità della rete non riguarda soltanto il fatto che si stende sull'intero pianeta ed è veramente oggi la forma estrema di globalizzazione. Internet è inseparabile. Non è solo un sistema di vasi comunicanti, è appunto una rete, per cui noi non possiamo pensare lo spazio economico di Internet come a qualcosa di separato; pensare alle regole del commercio elettronico senza perciò riflettere sugli effetti che tutto ciò potrà produrre, ad esempio su Internet come spazio sociale, su Internet come spazio pubblico per definizione.

Dobbiamo trovare quindi non solo regole specifiche per ciascuno di questi spazi, ma regole di compatibilità, che impediscano ad esempio alla dinamica economica che prende sempre più forza nella rete di oscurare, non voglio dire di cancellare, le potenzialità di Internet come grande spazio pubblico di confronto e di discussione.

Internet - lo accennavo - mette in discussione o crea identità individuali e collettive, modifica il ruolo dei soggetti, produttori e consumatori al tempo stesso, ci dà una nuova percezione di oggetti e contenuti della comunicazione, ci propone nuovi concetti.

Dunque si tratta di tenere insieme le diverse questioni e connetterle. L'idea di spazio pubblico si pone in maniera radicale, come luogo anche di costruzione della cittadinanza.

Noi non ci costruiamo in rete soltanto come consumatori, non ci costruiamo in rete soltanto come utenti di informazioni o produttori di informazioni, tendenzialmente ci costruiamo come cittadini; le analisi che sono state condotte, per esempio negli Stati Uniti attraverso ricerche sostenute in particolare dalla Mark Foundation, dimostrano la varietà degli usi civili di Internet, senza con ciò voler affermare che Internet è il luogo della democrazia. Internet, la rete per meglio dire, è una forma che la democrazia può assumere, è una opportunità per rafforzare la declinante partecipazione politica. È un modo per modificare i processi di decisione democratica.

Ma tutto questo ci riporta alla necessità di riflettere sulle precondizioni. Noi sappiamo che se vogliamo che l'affermazione altrimenti retorica della fine della distinzione tra soggetti produttori e consumatori di informazioni sia veritiera, sono necessarie almeno due condizioni che riguardano la connettività, e quindi le condizioni della connettività, i costi, le tariffe (tariffe telefoniche, questione particolarmente viva e importante in Paesi come l'Italia), le modalità e le regole dell'accesso e l'accesso non significa soltanto affermare genericamente o retoricamente che tutti possono accedere a tutto. A che cosa noi possiamo oggi accedere in condizioni di libertà? Non basta incidere sulle tariffe se poi ciò a cui accedo è sempre più costoso e se i beni e le informazioni a cui accedo liberamente sono sempre più limitate. Internet già ci mette di fronte a quello che può essere considerato un paradosso o una contraddizione. In teoria l'accesso è illimitato, in concreto la richiesta di accesso a costi particolari rischia di limitare molto tutto questo.

Voglio fare un esempio: può sorprendere o può essere considerato soltanto un fatto marginale, ma ai miei occhi è significativo, il fatto che due anni fa la Camera dei Lord in Inghilterra abbia ritenuto necessario intervenire, dichiarando una serie di manifestazioni sportive come una sorta di patrimonio culturale del popolo inglese, affermando che la finale

della Coppa di Inghilterra o il Torneo di Wimbledon o il Derby di Exon non possono essere trasmesse in forme criptate, debbono essere lasciate liberamente accessibili.

Esiste dunque un problema di una massa critica che deve essere mantenuta per evitare che l'accesso diventi soltanto formula retorica, potere di accedere, ma a che cosa e in presenza di quali condizioni?

Vi è poi il tema della alfabetizzazione informatica. Le condizioni di utilizzazione della rete sono oggi fortemente diseguali. Le diseguaglianze finora non sono diminuite, sono cresciute. Le ricerche fatte negli Stati Uniti dalla Rand Corporation, con riferimento a parametri come il reddito, l'istruzione, la collocazione sociale e la razza dimostrano che le distanze tra i vari gruppi in funzione di questi diversi fattori sono cresciute nell'ultimo decennio.

Naturalmente l'obiezione che viene fatta è che comunque siamo in presenza di tecnologie che per il loro carattere diffusivo invertiranno questa tendenza in tempi non lunghi.

Questo, tuttavia, non deve essere inteso come una sorta di non necessità di politiche pubbliche, per cui tutto può essere lasciato unicamente alle dinamiche di mercato, richiama invece la necessità di politiche pubbliche intelligenti e peraltro questo già sta avvenendo, con gli investimenti che nei diversi Paesi si fanno proprio in termini di alfabetizzazione di massa. L'alfabetizzazione non significa soltanto mettere un numero crescente di cittadini in condizione di usare un personal computer o di sapere come si accede a Internet, significa fornire la capacità di un uso critico di questi mezzi.

Nello stesso tempo però, Internet che può essere una grande opportunità e uno strumento di comunicazione e di coesione, si presenta anche, ed è una critica che tutti voi conoscete benissimo e sulla quale quindi non insisto, anche come uno strumento di frammentazione e di isolamento. La possibilità per ciascuno di noi di avere accesso rapido e diretto di comunicazione immediata con tutti coloro i quali si occupano dello stesso tema che ci interessa in qualunque angolo del mondo è certamente una straordinaria opportunità. Ma può diventare una gabbia, non la gabbia di acciaio di cui ci parlava Max Weber, ma certamente una limitazione nel senso che io, assorbito dalla comunicazione con gli studiosi della mia disciplina ai quattro angoli del mondo, perdo il contatto con gli altri studiosi di discipline diverse, che si trovano magari nella mia stessa facoltà universitaria, tutti chiusi nella loro stanza, a dialogare con i loro simili ma separati uno dall'altro. Ci sarà un'enorme crescita della specializzazione nei singoli settori, c'è il rischio della perdita della connessione con un paradosso che in questa materia diverrebbe inquietante.

Nello stesso tempo, la sfida che viene dalla rete è particolarmente rilevante ed evidente sul terreno della città politica. Gli spazi politici sono stati messi radicalmente in discussione. È ormai un luogo comune: quale che sia il libro, il saggio su Internet che apriamo, leggiamo tra le prime righe l'affermazione che i confini nazionali ormai non valgono più e che con essi è stata travolta la tradizionale sovranità degli Stati. Dunque uno degli elementi costitutivi dello Stato moderno che, come voi sapete, ha due elementi, ci raccontano gli studiosi: il popolo e il territorio.

Il territorio ormai è l'intero pianeta, il popolo dei cybernauti è l'umanità intera, almeno in prospettiva. Chi può governare una dimensione che abbia queste caratteristiche?

Naturalmente le tentazioni di utilizzare queste tecnologie, in modo non da arricchire, ma da impoverire i processi democratici è molto forte. Prima ancora dell'avvento di Internet si è molto discusso delle potenzialità delle tecnologie elettroniche per costruire la città democratica per eccellenza. I referendum elettronici sembravano il non plus ultra della democrazia. Abbiamo poi visto come essi possano diventare null'altro che la via alla manipolazione della partecipazione politica, il passaggio da una democrazia dei cittadini a una democrazia del plebiscito, in cui i cittadini saranno magari nevroticamente chiamati a votare tutti i giorni, ma esclusi dai processi di elaborazione politica.

Dunque, Internet ci offre la possibilità, aggiungerei l'obbligo, di riflettere invece su opportunità diverse. I cittadini non sono costretti a occuparsi soltanto del momento finale della decisione. Il sì o il no a una domanda che qualcuno dall'alto ci pone.

Il problema più importante non è essere associati al momento finale della decisione. Internet ci insegna - posso usare proprio questa parola - che è possibile cambiare il procedimento di elaborazione delle proposte, farlo diventare da procedimento chiuso in poche stanze o ristretto a poche persone, farlo diventare fatto corale. La valutazione dei progetti, la loro preparazione possono diventare fatto aperto a un numero tendenzialmente definito di soggetti, che possono intervenire più volte nel processo di decisione proprio perché non abbiamo più un processo piramidale, dove ciascuno può intervenire in un momento soltanto del processo di decisione, che poi sale a un livello superiore dal quale coloro i quali si trovano più in basso vengono esclusi, ma il procedimento a rete consente continui inserimenti nel processo di decisione. Questo è il punto su cui dobbiamo discutere: più che moltiplicare le possibilità di intervenire, quasi che la democrazia fosse un ininterrotto sondaggio solo nel momento finale della decisione.

La democrazia può diventare allora una democrazia continua, una democrazia che abbraccia l'intero processo di elaborazione e di decisione.

Si apre però in questo modo una sorta di conflitto tra usi sociali e usi commerciali di Internet, tra la richiesta di politiche pubbliche e invece la sottolineatura delle opportunità soltanto di regole private. Io insisto: dobbiamo liberarci da una visione puramente ideologica del problema e guardare in concreto quello che accade o che può accadere. Pensate alla questione dell'anonimato, in rete. È una questione capitale, come voi tutti sapete.

Qui vi è una significativa, importante convergenza tra le esigenze dello spazio sociale e politico, la libertà della discussione, l'ampiezza della partecipazione dei cittadini e le esigenze dello spazio economico, dove il commercio elettronico esige garanzie per gli utenti e per i partecipanti al processo di commercio elettronico, pena il rifiuto di questa dimensione. Se io vado in rete per acquisire beni e servizi senza la sicurezza per ciò che riguarda l'uso dei miei dati, evidentemente la dimensione del commercio elettronico può, già nel breve periodo, essere depressa o non avere la dinamica che ad essa si attribuisce.

Dunque, qui abbiamo una significativa convergenza intorno al tema del rispetto della privacy, della esigenza di anonimato nelle diverse dimensioni. Naturalmente con caratteristiche proprie, ma con un punto comune, vorrei dire con un denominatore comune di riferimento.

Qui ci accorgiamo che stiamo non dico dando un addio definitivo alla vecchia nozio-

ne di privacy, ma certamente possiamo cogliere con maggiore nettezza il fatto che da strumento di isolamento dagli altri, quale era l'antica nozione di privacy, diritto ad essere lasciato solo, la privacy diventa strumento di comunicazione. A me serve avere tutela dell'anonimato, a me serve la tutela della riservatezza della privacy non per isolarmi, ma per partecipare. Solo se sono certo del mio anonimato potrò partecipare senza timore di essere discriminato o stigmatizzato a gruppi di discussione in rete su temi politicamente sgraditi al potere dominante in un certo momento. Solo se avrò la certezza di non essere discriminato, potrò denunciare gli abusi, magari nel luogo dove io stesso lavoro.

Ecco allora che la riservatezza non è un problema di silenzio, di isolamento dagli altri, ma uno strumento di comunicazione. Allo stesso modo, nell'area del commercio elettronico, la riservatezza diventa lo strumento attraverso il quale, con fiducia, io accedo all'acquisto di beni o di servizi, avendo ad esempio la sicurezza che quelle mie informazioni non verranno ulteriormente utilizzate, fatte circolare, elaborate per costruire profili della mia personalità che potrebbero avere anche effetti discriminatori.

Tuttavia, quando noi ci preoccupiamo di questa dimensione, dobbiamo tenere conto che la dimensione della privacy non è da considerare soltanto da parte del soggetto attivo in rete, deve essere considerata anche dal punto di vista dei soggetti che possono essere a loro volta oggetto della comunicazione in rete. Mi spiego: se un imprenditore si sveglia tutte le mattine e trova in un sito particolarmente frequentato l'affermazione, che arriva da un anonimo, che questo imprenditore non è affidabile, consegna in ritardo, usa bambini per il lavoro, ecco, questa è sicuramente una affermazione che invade la sua sfera privata e se queste informazioni non rispondono alla realtà costituiscono sicuramente una invasione della sua sfera privata.

Ci troviamo quindi, in rete, di fronte alla esigenza di tutelare due diversi interessi alla privacy: da una parte l'interesse di chi comunica; dall'altra l'interesse di chi, essendo oggetto della comunicazione, ha diritto di vedere la propria sfera privata difesa da ingiustificate invasioni altrui.

E qui si pone un problema, come voi tutti sapete, molto delicato: arrivare al soggetto che immette in rete informazioni che possono violare la privacy altrui. Problema delicato perché incide con la questione dell'anonimato, pone il problema di quali siano gli obblighi del provider, se deve accertare in ogni caso l'identità di coloro i quali si servono della rete; come e con quali garanzie di segretezza deve conservare questa informazione su chi, essendo stato identificato all'ingresso, poi si manifesta in modo anonimo, con un nome di fantasia in rete, e in quali casi è legittimo superare il segreto, per quali esigenze e in base all'intervento di chi. Evidentemente una soluzione può essere quella di ritenere che solo con esplicito provvedimento dell'autorità giudiziaria e in presenza di rischi per la privacy o altri tipi di rischi per l'organizzazione sociale l'anonimato possa essere superato.

È un problema, ed è un problema che si ricollega poi alla questione della responsabilità dei providers. Voi sapete che è una questione aperta e io mi limito qui, poiché sarà certamente oggetto di ulteriori discussioni anche in questa mattinata, a segnalare soltanto un problema.

Se noi facciamo gravare un eccesso di responsabilità sul provider, sia responsabilità

penali che civili nel senso di farne i responsabili dei danni arrecati a coloro i quali usano la rete, noi, consapevoli o meno, possiamo avviare dei processi di censura.Se il provider sa che, ammettendo in forme anonime, che non potranno essere superate, alcuni soggetti in rete, che arrecheranno danni a terzi, sarà poi il provider a doverne rispondere perché non potrà essere superata la barriera dell'anonimato, il provider, per ovvie ragioni di autodifesa, selezionerà in modo molto rigoroso non solo coloro i quali sono inaffidabili dal punto di vista economico, ma anche quelli che possono apparire scomodi o pericolosi per le opinioni che esprimono.

Quindi noi affermiamo in astratto la libertà della rete, ma facciamo del provider un censore istituzionale e rischiamo in questo modo di entrare in contraddizione con un altro dei caratteri che alla rete viene attribuito, quello di essere un potente strumento di disintermediazione. Si dice: la possibilità del contatto diretto, superare gli intermediari tradizionali.

È vero, la comunicazione, punto a punto. Ma se noi, di questo intermediario tecnico, che è il provider, facciamo anche un intermediario sociale, un filtro giuridico, ricostituiamo condizioni di intermediazione in modo sicuramente pericoloso.

Qual è la via da seguire, allora? In questi anni i tentativi di cogliere la dimensione sociale, economica, giuridica di Internet hanno spinto in molti casi ad analogie con altri schemi già noti. Questo è del tutto ovvio. La novità sconvolge in molti casi; sfida poi la pigrizia dei giuristi, i quali sono molto restii in molti casi ad abbandonare gli schemi ai quali sono affezionati e che danno loro certezza. Ecco che si è detto: la rete è molto simile alla disciplina dell'ambiente. Anche lì, nell'ambiente c'è un danno che ha la sua origine in un luogo lontano e che si propaga senza rispetto delle barriere nazionali. L'inquinamento del Danubio, che attraversa una serie di Paesi; le foreste di questo o di quello Stato danneggiate dalle piogge che hanno origine in uno Stato lontanissimo; l'inquinamento delle nevi delle Alpi per effetto della sciagura di Chernobyl, non ci dicono qualcosa che ci riporta proprio alla rete, dove i fenomeni hanno origine in un luogo, effetto in un luogo lontano, diverso dal punto di vista dello Stato interessato, e ciò quindi pone gravi problemi per stabilire quale sia il soggetto competente a intervenire, quale sia la regola da applicare.

Ancora: analogie tratte dal diritto della navigazione. L'alto mare è un luogo che non è soggetto alla sovranità degli Stati, o il diritto dell'Antartide, come un luogo senza sovranità statuale, regolato da intese tra i diversi Stati, e ancora la suggestione della *lex mercatoria*, la legge creata spontaneamente dai rapporti tra mercanti nel Medio Evo. In una situazione in cui le frontiere erano attraversate con molta maggiore libertà di quanto avvenga oggi;

Marco Polo probabilmente arrivò fino alla Cina senza dovere esibire mai un passaporto.

Quindi, lo schema che affascina qualcuno anche dal punto di vista linguistico, invece di *lex mercatoria*, in saggi, non nell'ambiente giuridico italiano affezionato al latino, ma negli Stati Uniti, hanno come titolo *lex informatica*.

Tutte queste analogie con il passato colgono certamente aspetti veri della natura e della dimensione di Internet, ma solo qualche aspetto. La dimensione globale non è colta da queste analogie, che quindi, spinte oltre un certo limite, possono diventare anche un ostacolo a una corretta impostazione della questione istituzionale di Internet.

Certo, la sovranità nazionale è finita. È finito quello che si è chiamato il territorio giacobino. Lo Stato moderno si è retto sull'idea di un territorio chiuso nei confini, governabile da un unico centro, dall'alto. Oggi ci troviamo di fronte all'assenza di confini, ma anche alla creazione di entità diverse dagli Stati, a diversi soggetti che da punti diversi intervengono per regolare il traffico in rete, e quindi la prima questione è la ricognizione della complessità dei diversi centri di potere che regolano questo universo.

Non possiamo più pensare che sia soltanto una la sede della regolazione. Su questo, credo che si vada creando un consenso piuttosto diffuso, che taglia da una parte gli assertori invincibili della libertà anarchica in rete, e dall'altra i sostenitori dell'altrettanto invincibile logica della regolazione da parte di un unico centro: lo Stato o altro che sia.

La logica è piuttosto quella che io chiamerei di una strategia integrata, che vede presenti soggetti e strumenti diversi, che io elenco con estrema rapidità, cercando di concludere questa mia introduzione.

Atti internazionali e sovranazionali, di varia provenienza, convenzioni, ma non soltanto. Pensate in questo momento allo sforzo che sta facendo l'OCSE di rivitalizzare le sue linee direttive del 1981, per adattarle alla nuova grande dimensione di Internet. Le norme nazionali, di vario rango; l'intervento dei giudici, che nell'ultimo anno ha, soprattutto in Paesi come gli Stati Uniti, manifestato una particolare vitalità e dato maggiore concretezza alla riflessione proprio sui problemi giuridici di privacy. I codici di deontologia, richiamati anche esplicitamente dalla direttiva europea 95/46. Le certificazioni da parte di soggetti. Il ricorso ai contratti. Gli standard tecnici, le *privacy enhancing technologies*, che costituiscono anche qui una sorta di modello linguistico che si ritrova altrove. La ricerca più interessante che io abbia letto negli ultimi tempi, proprio un mese fa, si intitola *Democracy enhancing technologies*, dove il calco linguistico è proprio quello del PET, delle *privacy enhancing technologies*.

Vorrei dire rapidamente pochissime cose su questo punto capitale, perché in questo momento l'accento posto proprio sulle tecnologie protettive dei diritti della privacy in primo luogo è molto forte e tende in molti casi ad essere presentato come un approccio al problema che esclude tutti gli altri, nel senso che l'arricchimento dello strumentario tecnologico può rendere inutile, superfluo o del tutto accessorio il tipo di regola giuridica o comunque norme statuali e perfino norme deontologiche.

Io credo che qui la questione sia particolarmente importante. Dobbiamo renderci conto che le *privacy enhancing technologies* non costituiscono la risposta a un problema tecnico.

Herbert Burkert insiste e ci richiama sempre alla necessità di riflettere su questo punto. Sono un tentativo di rispondere a un problema politico e sociale, dunque non possono essere descritte all'insegna della neutralità.

Faccio soltanto un esempio - avremo in questi giorni opportunità di valutare tutti questi aspetti, io non anticipo soluzioni, non voglio invadere i campi degli altri relatori, richiamo soltanto alcuni problemi. Quando noi insistiamo, con particolare attenzione e intensità, sulla opportunità di tecniche di filtraggio per tenere al riparo i minori dall'accesso a informazioni e a siti che possono rappresentare un rischio per essi; a tecniche di filtraggio per ciò che riguarda i siti nei quali si manifestano violenza, discriminazione razziale, il nega-

zionismo che sta invadendo alcune reti negli Stati Uniti per tutto ciò che riguarda, per esempio, la vicenda nazista, apparentemente ci dotiamo di strumenti tecnici che danno una risposta soddisfacente a esigenze socialmente diffuse. Ma noi non ci rendiamo sempre conto - anche se ormai il problema è sottolineato con grande intensità - che stiamo creando nuovi, accentrati e incontrollati centri di potere, perché il potere di classificare l'informazione come violenta diventa in quel momento il potere socialmente più rilevante perché se a quella classificazione corrisponde poi sul mio software un segnale per cui automaticamente io vengo escluso dall'accesso a quel tipo di informazione, voi vi rendete conto, immediatamente, delle conseguenze sociali e politiche di questo tipo di classificazione. Non è né innocente né neutrale il ricorso a queste tecnologie. Va valutato per il quadro istituzionale all'interno del quale si inserisce, ma le polemiche intorno al *Communication Decency Act*, al *Wchip* e a tutto ciò che ha questa caratteristica, alla crittografia non ci dicono proprio che entriamo su un terreno socialmente e politicamente assai sensibile, di cui vanno ridefiniti i termini e i confini. Non siamo di fronte a tecnologie neutre, neutrali; siamo di fronte a tecnologie in cui si manifesta al massimo grado la forza di modello sociale della rete e quindi esigono una seria discussione sul quadro istituzionale, all'interno del quale noi possiamo muoverci e dobbiamo muoverci.

Tutto questo mi porta a dire, anche se in passato molte volte, ancora nella relazione che ho fatto all'inizio di quest'anno all'OCSE, mi limitavo a dire: ci troviamo di fronte a tutte quelle forme e a tutti quei soggetti che possono intervenire, si tratta di integrarli opportunamente. Ma prima di integrarli, è necessaria una riflessione accurata su ciascuno di essi.

Le *privacy enhancing technologies* richiedono questo tipo di riflessione; il riferimento alle norme giuridiche richiede altrettanta riflessione critica. Che tipo di norme giuridiche?

Norme giuridiche di tipo stringente o norme giuridiche elastiche, capaci di autoadattarsi alle situazioni che cambiano? Questa è una domanda alla quale dobbiamo rispondere.

E poi, anche all'interno delle stesse tecnologie, del filtraggio, comincia a porsi il problema, ma noi non rischiamo di introdurre un elemento di rigidità. Che tipo di rigidità introduciamo quando stabiliamo un rapporto tra codici, che riflettono valori e che escludono poi l'accesso a determinati siti? E se cambia la valutazione sociale? Quali interventi dovranno essere fatti sui software? Quali costi, anche economici, dovranno essere sopportati?

Problemi tutti che richiedono non solo la considerazione del fatto che ci sono diverse tecniche che devono combinarsi, ma del fatto che queste tecniche, entrando nella nuova dimensione, trovano sicuramente una ridefinizione.

Dobbiamo fare due operazioni contemporaneamente. Per i codici deontologici, ad esempio - e bisogna dirlo, credo con sincerità - finora hanno funzionato poco. Sono codici di prima generazione, in qualche caso, se li leggiamo, poverissimi di contenuto normativo, sono più delle dichiarazioni di intenzioni. Sono più degli strumenti che hanno una finalità di prima rassicurazione di angosce sociali che veri e propri insiemi di regole. Infatti chi riflette su questi temi si chiede se siamo di fronte a quella massa critica necessaria perché i codici deontologici possano pesare effettivamente come strumenti di regolazione.

Concludo: qui ci troviamo di fronte a diversi problemi, che ho cercato sommariamen-

te di indicare, non li ho indicati tutti, ne ho indicati alcuni e vorrei concludere con una considerazione.

Io dico qualche volta, scherzando, che quando riflettiamo su Internet dobbiamo fare i conti con tre P: pornografia, privacy e proprietà. La pornografia è un problema, ma può diventare anche lo strumento per introdurre forme di censura. La risposta della Corte Suprema americana al *Communication Decency Act*, quale che sia il modo in cui noi la valutiamo, è sicuramente l'espressione di queste preoccupazioni. E ci dice anche un'altra cosa: che noi abbiamo bisogno, in primo luogo, di principi di riferimento molto forti: possiamo articolare come vogliamo i diversi strumenti. Ma quali sono i principi di riferimento? Non sempre è indispensabile riscrivere questi principi di riferimento. La Corte Suprema degli Stati Uniti, come sapete tutti, ha basato la sua decisione sul *free speech*, sulla libertà di manifestazione del pensiero, 1° emendamento della Costituzione americana, approvato il 25 settembre 1789. Quando i principi sono forti, socialmente condivisi, non è la data di nascita a contare, ma i principi sono necessari. Per Internet come per tutti gli altri aspetti della vita democratica, noi abbiamo bisogno di un quadro forte di principi di riferimento, all'interno del quale poi troverà posto, in una logica non più monocentrica, ma corale, una molteplicità di soggetti e di strumenti.

Privacy, non ho bisogno di insistere su questo punto: è uno dei grandi terreni di verifica non solo della efficienza di Internet, ma anche della sua capacità democratica. Se tutela della privacy significa nello stesso tempo dinamica economica e partecipazione politica, è chiaro che qui si gioca l'una e l'altra.

Proprietà: noi avremo questo pomeriggio un discussione molto impegnativa, ma evidentemente la estensione senza ragioni solide della logica proprietaria a tutti gli oggetti che possono essere portati in rete, può comportare restrizioni forti dello stesso diritto di sapere.

L'enfasi posta tante volte su Internet come la biblioteca totale - non dirò la biblioteca di Babele di Borges - rischia di essere vanificata proprio dalla logica proprietaria. La biblioteca pubblica nella storia della civiltà, dalla biblioteca di Alessandria distrutta dall'incendio, fino alla *très grande bibliothèque* di Mitterrand, è l'accesso libero e gratuito di tutti al sapere. Internet non può diventare il luogo dove alcuni acquistano i diritti sui musei e subordinano poi al pagamento di un pedaggio la possibilità di accedere da lontano alla visione della Gioconda o della Primavera di Botticelli.

Stiamo discutendo sicuramente di dati molto concreti, ma stiamo anche disegnando o ci stiamo interrogando intorno al futuro della cittadinanza democratica.

Prof. Giuseppe Santaniello

Esprimo un vivo ringraziamento e apprezzamento al Prof. Rodotà per la sua relazione introduttiva. Tra i tanti pregi che hanno connotato la sua analisi ve ne è uno assolutamente preminente: la relazione ci ha offerto i punti cardinali, perché ognuno di noi si possa orientare in un sistema complicato quale è il sistema Internet.

Il prof. Rodotà ha trattato i punti fondamentali, i momenti fondamentali del tema, in particolare i poteri, le figure soggettive, gli operatori, gli utenti del sistema Internet.

Vorrei ricordare che la sua relazione è un ulteriore contributo scientifico che si aggiunge ai tanti apporti in sede dottrinale, in sede politica, in sede parlamentare, in sede mediatica che Rodotà ha dato per formare la cultura della informazione e della privacy.

RISERVATEZZA E SICUREZZA DELLE RETI

Prof. Yves Poullet
Faculté Universitaire Notre-Dame de la Paix - Namur

Je voudrais d'abord remercier mon ami Stefano Rodotà et tous les organisateurs de cette rèunion de m'avoir invitè dans un lieu dont le prestige est à la hauteur des dèfis que la sociètè se doit de relever lorsque l'on parle des problèmes d'Internet. Je vous remercie ègalement d'avoir insister pour que je m'exprime dans ma langue.

Je voudrais èvoquer trois problème. Le premier c'est d'essayer de vous montrer quels sont les nouveaux risques liès à l'utilisation d'Internet, nouveaux risques en ce qui concerne la protection des donnèes. Je voudrais ensuite me risquer sur l'analyse des solutions. On a dèjà èvoquè les PET, les privacy enhancing technologies, je voudrais en dire un mot, les dètailler, parler ègalement des systèmes d'autorègulation qui existent et de voir enfin - et ce sera la troisième partie - la manière dont Internet remet en cause les directives en matière de protection de donnèes.

En ce qui concerne les nouveaux risques liés à l'utilisation d'Internet. Je crois qu'il suffit d'évoquer à cet égard les quatre caractéristiques d'Internet.

La première c'est qu'Internet est un réseau ouvert, cela veut dire que chacun peut s'y connecter et que d'autre part chacun peut s'y connecter pour les utilisations qu'il souhaite faire et qui ne sont pas nécessairement les utilisations auxquelles celui qui a placé des données sur Internet avait réfléchi. En d'autres termes, il va de soit que si tout le monde peut avoir accès il y aura des problèmes de confidentialité du réseau, si chacun peut utiliser les données comme bon lui semble, il y aura la possibilité par exemple, grâce aux robots de recherche, de pouvoir identifier, sans aucun problème le profil d'une personnalité à travers sa présence dans un certain nombre de groupes de discussion ou à travers les sites dans lesquels elle est présente.

Deuxième réflexion en ce qui concerne le caractère ouvert du réseau: c'est le fait que, grâce au hyperlink, je peux sauter d'un site web à un autre site web; cela comporte un risque, c'est que tous ces sites web, comme il sera dit plus tard, sont interconnectés et ils peuvent garder des traces de mon parcours sur Internet. Chaque site peut savoir d'où je viens et où je vais et si je prends certains acteurs comme les fournisseurs d'accès,ils peuvent avoir une vue complète de mon type d'utilisation d'Internet.

La deuxième caractéristique c'est certainement le fait qu'il s'agit d'un réseau interactif. Internet crée un nouveau problème du fait que je suis moi-même le générateur par mon utilisation de mon navigateur d'un certain nombre de données. C'est moi qui en visitant tel

ou tel site crée des données nominatives. Le fait que tel jour j'ai visité tel site et à l'intérieur de ce site telle page, par exemple à l'intérieur du Washington Post, j'ai été particulièrement intéressé par la page de sport; le fait que de là je suis passé à une agence de voyages, que je me suis intéressé aux voyages relatifs à l'Afrique, etc., etc., le fait que j'ai été visité sur un site web les précautions aussi concernant le SIDA.

La caractéristique suivante est certainement le fait qu'il s'agit d'un réseau international.

Pas de frontières pour Internet, cela veut dire que l'on peut côtoyer un certain nombre de pays où existent des protections, des réglementations fortes de protection et d'autres pays où il n'existe aucune réglementation. Une chose qui est extrêmement simple, c'est de pouvoir délocaliser un site et donc à partir de ce moment là si un pays offre une réglementation trop contraignante, il est facile de le déplacer vers un pays où aucune réglementation n'existe.

Enfin, la dernière caractéristique c'est le fait que Internet se caractérise par une multiplicité d'acteurs. Dans le cadre d'une recherche qu'actuellement nous menons, qui s'appelle Eclip et que nous menons pour la Commission Européenne, nous avons essayé d'établir une espèce de typologie d'acteurs et de typologie d'opérations en ce qui concerne une opération très simple, l'opération d'acquisition de biens sur Internet. Et vous voyez le nombre d'acteurs qui peuvent intervenir, pas simplement celui qui va vendre le bien, mais également le carrier, le transporteur du message, qui peuvent être nombreux, une compagnie de cyber-marketing - je reviendrai là-dessus - le fournisseur des services Internet, la banque; on peut ajouter le fournisseur d'accès à Internet. Chacun de ces acteurs va à un moment donné pouvoir collecter des données. Nous avons listé le type de données que chaque acteur peut connecter.

Voilà un certains nombres de risques qui sont liés aux caractéristiques générales d'Internet. Je voudrais, et je le fais rapidement, vous montrer que au-delà de ces risques il en existe d'autres, ce qui naît du fait qu'Internet n'a pas simplement sa face visible, mais qu'il a également une face cachée, un certain nombre de traitements existent à l'insu de l'internaute. Ce sont d'abord des traitements qui ont lieu au niveau de ce qu'on peut appeler les couches transports, les couches basses dans le sens du modèle ISO, à savoir le modèle en ce qui concerne la standardisation des réseaux de télécommunications.

Là il y a pas mal de traitements cachés. Il y a le fait d'abord que en ce qui concerne la voie de transport, il ne faut pas penser que entre deux villes proches, Namur et Bruxelles (nous avons fait l'expérience) le chemin emprunté sera le chemin le plus court, 60 km. Notre message, partant de Namur passera par le transporteur situé en Suisse, à Genève, à Helsinki, à Paris, voire à Washington.

Le deuxième risque c'est le fait qu'il est possible, grâce à des manipulations de non-demain, ce qu'on appelle le "web spouting", de faire en sorte que le site web par lequel vous accédez ne soit pas exactement le site auquel vous souhaitez accéder mais une espèce de site en trompe-l'oeil, ce qu'on appelle un site miroir, et récemment un site web belge a fait l'objet d'une perquisition et de sanctions pénales parce qu'il avait créé artificiellement un site qui reproduisait le site d'un journal et qui bien évidemment était un faux site mais qui lui permettait d'obtenir des données et des données personnelles en particulier.

La commande ..... c'est une spécificité du réseau qui permet de savoir si à un moment

donné un autre internaute est connecté au réseau et utilise sa connexion c'est une manière indiscrète de savoir si vous êtes en train d'utiliser une version moderne du téléphone.

Voilà en ce qui concerne les risques invisibles liés aux couches que l'on peut considérer comme les couches les plus basses.

En ce qui concerne les couches les plus élevées il y a d'autres traitements non pas visibles, comme il est indiqué, mais invisibles, il y a d'autres traitements qui sont possibles et en particulier ceux qui sont liés à l'existence des cookies. Qu'est-ce que c'est que les cookies? Ce sont simplement des morceaux d'information, mais ça peut être plus, ça peut être carrément des parties de programme qui sont envoyés sur votre navigateur lorsque vous êtes connectés à un site web et qui vont permettre à ce site web, chaque fois que vous vous reconnectez à lui de pouvoir vous reconnaître en tant qu'utilisateur. En d'autres termes, si je me suis un jour connecté au site web du Washington Post et que le Washington Post m'a envoyé un cooky, chaque fois que je vais me connecter à Washington Post, Washington

Post pourra savoir qu'il y a trois jours, il y a un mois, il y a deux mois je me suis connecté et les pages précises que j'ai lues à ce moment.

Les objectifs? Il est clair que les objectifs peuvent être considères dans une certaine mesure comme légitimes lorsqu'il s'agit d'assurer la continuité du service. Il arrive que le réseau Internet soit à un moment donné interrompu, coupé et que dès lors il est peut être intéressant de pouvoir reprendre la transaction là où vous l'aviez arrêtée. Le cooky le permet; le site web peut vous reconnaître et à partir de ce moment-là reprendre la transaction là où on l'avait arrêtée.

Il y a des objectifs qui sont moins propres et je pense en particulier à l'objectif du marketing individuel.

L'idée est la suivante. C'est que plutôt qu'avoir des publicités qui sont des publicités que l'on envoie à l'ensemble d'une population, et qui ne sont pas ciblées sur une personne particulière, l'interactivité d'Internet permet d'ores en avant de connaître exactement les préférences de chaque utilisateur et de lui envoyer la publicité qui convient. A cet égard des sociétés de cyber-marketing, comme Double-click, qui a plus de 2.500 compagnies déjà affilées, et ce nombre est véritablement en explosion, des sociétés de cyber-marketing vont collecter des données d'utilisation d'Internet à partir d'un certain nombre de sites qui sont affiliés à cette société et à partir de ce moment-là vont pouvoir, sur la base de cette collection étendue, mieux cibler quelles sont les préférences de chaque internaute.

Si vous me permettez, je vous décris rapidement le fonctionnement. Lorsque je me connecte à un site-web, je pense par exemple au site d'Altavista, nous avons fait l'expérience à plusieurs reprises et ça fonctionne véritablement très bien ou très mal suivant les points de vue.

Lorsque je me connecte au site d'Altavista pour faire de la recherche pour tel nom ou éventuellement sur tel mot, Altavista a un hyperlink, un lien automatique avec Double-click; ce qui veut dire que lorsque je me connecte à Altavista, automatiquement la société de marketing va m'envoyer un cooky et va automatiquement, recevoir un certain nombre d'informations. D'abord des informations que de toute façon je veux mettre dans mon entête: des informations relatives à la page que je suis en train de visiter, le fait que le cas échéant un

cooky à déjà été envoyé sur mon navigateur, le fait que j'utilise tel type de navigateur - Netscape, quelle version - et que j'utilise cela sur un OS de telle génération et puis l'adresse de l'internaute. Cette adresse n'est pas stable, n'est pas fixe et donc peut être considéré qu'il ne s'agit d'une donnée personnelle, mais la question est posée en ce qui concerne l'information générée par le cooky, car avec ce cooky la société à laquelle la société de marketing et l'Altavista vont savoir non pas qui je suis, nous ne saurons pas l'utilisateur qui est derrière le navigateur, mais en tout cas ils sauront, et cela avec certitude, ce que cet utilisateur fait.

Voilà ce que je souhaitais dire en ce qui concerne la manière dont fonctionnent les sociétés de cyber-marketing qui à mon avis représentent un problème grave.

En conclusion de cette réflexion sur les traitements invisibles, je voudrais ajouter qu'il y a une différence, et une différence nette, entre ce que l'internaute croit faire et ce qui se passe réellement.

Quelle est votre impression lorsque vous vous connectez à des sites web? C'est que chacun de ces sites est quelque chose d'autonome, qu'il n'y a pas d'interrelations entre ces sites. Lorsque vous vous connectez à Altavista, vous croyez sortir d'Altavista et aller vers un site 1, puis vers un site 2, vers un site web 3, en réalité ce qui se passe est tout autre.

Trois réflexions à cet égard. Premier point: tous les sites que vous visitez sont interconnectés, c'est-à-dire que chaque site que vous visitez garde une trace du site que vous avez visité précédemment et garde une trace bien évidemment du site vers lequel vous allez. Une première donnée nominative qui peut être intéressante. Il vient de telle page, les Trois Suisses, et il va vers telle page, à savoir la Gazette des Sports.

Deuxième réflexion: dans la mesure où ces sites sont affiliés à un NTTP, comme une société de cyber-marketing. Pourquoi NTTP? Parce que nous avons voulu jouer sur les mots, à savoir Not Trusted Third Party. C'est un tiers qui n'est pas de confiance, qui va collecter des informations sans vous en avertir. Eh bien, celui-ci va, dans la mesure où Altavista et le site 1 sont connectés à lui, chaque fois pouvoir connaître le type d'utilisation que vous faite de ce site.

Tout cela est permis et je trouve qu'on n'a pas été suffisamment attentifs à cela: on parle beaucoup de réglementation de fournisseurs d'accès, on parle de réglementation de Internet Access Provider, on n'est peut-être pas assez attentifs au fait que ce qui permet tout cela c'est bien évidemment le navigateur, le fait que le navigateur va permettre l'envoi du cooky, va faire en sorte que, automatiquement, de par l'utilisation de notre browser, tout cela va faire en sorte que les possibilités d'utilisation des données qui m'apparaissent comme en tout cas déloyales seront possibles.

Ayant vu les risques, je voudrais réfléchir avec vous sur quelques solutions auxquelles on peut songer pour bien évidemment éviter ces risques. Mais avant d'analyser ces solutions, les solutions techniques, les solutions d'autorèglementations, les solutions légales, je voudrais poser trois questions qui m'apparaissent fondamentales. Pour chaque solution, il me semble qu'il faut se poser trois questions.

La première question: celle de la légitimité de la solution qui est proposée. Légitimité, ça veut dire de savoir si l'auteur qui propose cette solution est légitimement autorisé à la

proposer; ça ne veut pas nécessairement dire que ça doit être un auteur constitutionnellement désigné, mais ça ne veut certainement pas dire en tout cas que la légitimité implique qu'il y ait une discussion ouverte, qui permet de prendre en considération le point de vue, y compris des premiers intéressés, des internautes, et l'on peut s'interroger sur la légitimité d'un certain nombre de solutions d'autorèglementation à cet égard.

Deuxième point qui m'apparaît important c'est le fait que la solution doit être conforme, la conformité c'est le fait me semble-t-il qu'il doit y avoir *compliance*, il doit y avoir adéquation avec les principes en matière de protection de données, il reste à les définir.

Enfin, cette autorèglementation est un trompe-l'oeil si elle n'est pas effective. Et pour savoir si ellr est effective il faut vérifier si l'autorité qui va établir l'autorèglementation, ou éventuellement des tiers qui sont chargés du respect de la réglementation disposent des moyens nécessaires, s'ils ont la possibilité de sanctionner et quel type de sanction.

Dans les différentes solutions, la première c'est celle dont tout le monde parle, c'est certainement la solution technique. J'ai repris la définition de Herbert: les faits ce sont des constructions, des devices techniques qui font en sorte que l'on va essayer soit de minimiser soit de faire en sorte qu'il n'y ait pas de traitements de données personnelles.

Qui est-ce qui existe à cet égard? Le PET c'est ce que George Heiderbeg a appelé, dans un article qui a fait beaucoup de bruit outre Atlantique, la *lex informatica* dont il voyait un certain nombre d'avantages par rapport à la lex classique. Deux types de niveaux en ce qui concerne les PET. D'abord, premier point, un certain nombre de techniques qui vont permettre la protection des données se situent au niveau de l'anonymité et de la confidentialité du message. C'est de faire en sorte que quelqu'un puisse envoyer un message de manière anonyme et que ce message circule de façon sûre. Le premier Pet c'est évidemment l'utilisation de techniques de cryptage. Je vous rappelle que le Berlin Working Group qui travaille sur la privacy des télécommunications avait recommandé dès 1995 alors que le débat relatif au cryptage commençait que l'on puisse librement utiliser des techniques d'encryptage de façon à permettre qu'il n'y a ait pas atteinte à la confidentialité des messages.

Deuxième type de services - c'est le cas de M. ..... en Finlande - qui avait offert des services d'anonymisation, c'est-à-dire des services de postage anonyme qu'il utilisait simplement pour faire en sorte que le site web ou que votre correspondant ne puisse pas savoir qui est l'émetteur du message, vous passez par un tiers, qui va faire en sorte, qui va vous donner une adresse *just in case*, adresse qui vous permettra bien évidemment de ne pas être reconnu par la personne à qui vous envoyez le message, c'est un système où on va vous fournir une espèce de masque d'identité.

La dernière possibilité est ce qu'on appelle le surfing anonyme. L'idée du surfing anonyme prend de plus en plus de poids. Lors de la dernière réunion du groupe de Berlin deux réflexions ont été faites. Premier point: l'affirmation que les browsers, les navigateurs de Netscape, votre Microsoft Explorer, devaient vous permettre de pouvoir naviguer anonymement, ce serait extraordinaire, c'est-à-dire ne pas révéler qui vous êtes. Et deuxième recommandation qui a été affirmée, qui m'apparaît importante, c'est la possibilité pour tous de pouvoir passer par des pseudonymes. Je crois que c'est un point important de ne

pas devoir signer soi-même, en tant que personne identifiée, mais de pouvoir signer sous le masque d'un pseudonyme. Ce sont deux recommandations qui certainement devront être suivies.

Lorsqu'on parle des PETS on évoque bien évidemment surtout les développements actuels, en termes de réflexion, mais aussi en termes d'implémentations technologiques, réflexions actuelles qui sont réflexions du *plate-forme for privacy* préférence. L'idée est la suivante: il s'agit d'implémenter, dans le domaine de la vie privée, les solutions qu'on a évoquées ce matin, les solutions qu'on a évoquées en matière de messages obscènes ou de messages pornographiques. L'idée est de dire: utilisons le système PICS - *Platform for Internet Content Selection* - mais utilisons-le de manière à permettre la protection de la vie privée et non plus simplement la protection des messages obscènes ou autres.

Ces technologies ont été développées par le *World Wide Web Consortium*, vous voyez il y a la fois un interlocuteur américain, un interlocuteur français et un interlocuteur japonais, ici vous pouvez trouver toutes les informations, simplement pour vous dire que toutes les sociétés, Microsoft, Netscape, IBM, Compaq, mais également Double-click, les grands server sont présentes dans ce consortium et participent à ce consortium.

L'idée est la suivante, je la résume autour de quatre acteurs. Premier acteur ce qu'on peut appeler l'autorité de la labellisation qui va spécifier a priori le contenu de label et leur signification. Si je dis qu'une société est conforme à la protection des données qu'est-ce que ça signifie? En termes d'abord de savoir ce qu'est une donnée personnelle. Qu'est-ce que ça signifie en termes d'utilisation légitime de cette donnée. Est-ce que cette société est conforme parce qu'elle utilise pour elle-même, parce qu'elle utilise éventuellement pour des finalités uniquement de tarification, ou bien est-ce qu'elle est conforme parce que même si elle communique, elle permet au tiers d'avoir un droit d'accès.

La première question qui va être posée à l'autorité de labelisation c'est de dire: définissez-moi une terminologie qui permette a priori de savoir que lorsque vous dites que tel site web offre une protection de type 2, eh bien qu'on sache ce que veut dire cette protection de type 2, en termes de télé, de conservation de données, en termes bien évidemment de type d'utilisation, en termes bien évidemment de droit d'accès.

La première chose c'est de développer un vocabulaire commun et je vous jure que c'est un problème extrêmement délicat, extrêmement difficile, la commission française a fait à cet égard un certain nombre de premières réflexions sur le vocabulaire utilisé par P3P.

Deuxième idée, c'est de faire en sorte qu'on puisse connaître la situation de label. Qu'est-ce que ça veut dire label en matière de protection de données? Qu'est-ce que ça vaut dire label 2 en matière de protection de donnés? etc... etc..., il faut assurer une large diffusion.

Deuxième acteur - et c'est évidemment l'acteur le plus délicat - une fois que le vocabulaire aura été défini, qui va auditer le site web et qui va dire: ce type de site web correspond au label de type 1, 21 ou 3. Cette autorité peut être le site web lui-même, ce qu'on appelle le *self-rating*, ou cela peut être une autorité tiers, à savoir, par exemple, une société d'accountants qui le fera pour le compte du site web.

Une fois que le label a été délivré on va publier. Tel site web a un label de type 1, 2 ou 3.

Qu'est ce qui reste à faire? Il reste le rôle de ce qu'on peut appeler le software company et en particulier les compagnies qui développent des navigateurs. Elles doivent permettre me semble-t-il deux choses. Elles doivent permettre que le navigateur soit configurer de telle sorte que l'internaute puisse exprimer cette préférence, puisse dire: moi, je veux absolument un niveau de protection de données de type 7, le niveau le plus fort.

Et puis deuxième point: une fois que j'ai configuré mon navigateur avec le label de type 7, il faut bien évidemment que mon navigateur puisse, lorsqu'il rencontre un site web qui ne veut pas un niveau de protection de type 7 ou qui a simplement un niveau de protection inférieur, et bien, qu'il puisse bloquer l'accès à ce site. Ou, c'est en cela évidemment qu'il y a un gros progrès par rapport à la technologie X au départ ou qu'il puisse offrir à l'internaute qui se rend compte que le site web auquel il va accéder n'a pas le niveau de protection qu'il aurait souhaitable à priori, qui puisse permettre à cet internaute éventuellement d'entrer en négociation. On dit: voilà vous ne ferez pas telle protection, moi je réclame telle protection, qu'est-ce que vous pourrez m'offrir comme garantie supplémentaire?

Voilà ce que l'internaute, le quatrième acteur doit pouvoir faire, soit le site web, est du même niveau de protection, pas de problèmes, c'est ce qu'on appelle l'automatic matching, soit il n'est pas du même niveau et à ce moment là c'est la négociation.

Bien de choses sont encore à dire, je ne veux pas développer un point sur lequel nous pourrions revenir, qui est le problème de la régulation des navigateurs, sur ce point là notre équipe de recherche a fait un certain nombre de recommandations, qui ont été présentées à la conférence européenne des agents de protection des données. On peut revenir tout à l'heure sur ce point.

En ce qui concerne l'autorégulation. L'idée est dans le cadre d'un système de normalisation. On ne pourrait pas a priori définir des modes de gestion de données nominatives qui seraient respectueux des principes de protection des données. La *self régulation*, c'est en cela que je l'ai distinguée des PETS, met plus l'accent sur les modes de gestion, alors que le PETS met l'accent bien évidemment sur des technologies qui a priori interdiront tel ou tel mode de gestion. Dans le cadre de l'approche ISO l'idée très nette est de dire: nous allons essayer de définir des modes de gestion de l'information à l'intérieur des entreprises qui offrent des services par Internet qui puissent être correspondant à des principes de protection des données.

C'est un travail qui a commencé dans le cadre de l'ISO par le *Consumer policy committee*, c'est intéressant de voir quels sont les consommateurs qui se sont montrés intéressés par ce système et qui ont été les premiers à intéresser par le développement de cela.

Ce système est un système qui bien évidemment repose sur un certain nombre de procédures, puisque le problème va être, une fois que l'on a défini une certaine liste de pratiques en matière d'utilisation correcte de l'information, de pouvoir dire que tel site web est bien conforme à ce standard qui a été défini une fois pour toutes.

Donc le problème qui va se poser est comment régler la question des procédures d'accréditation des citoyens. Comment est-ce qu'on va faire pour qu'un site web soit reconnu comme conforme.

Première question, nous travaillons avec des sociétés d'accountants pour essayer de voir comment on pourrait faire. Première question qui nous est renvoyé c'est de dire: est-ce que l'accréditation, et ça c'est un petit peu la même chose que dans le cadre de P3P, est-ce que l'accréditation est faite par le site web lui-même, bien qu'elle doit être faite nécessairement par une entreprise tiers qui est habilitée à auditer le fonctionnement de l'entreprise. C'est un problème qui est extrêmement délicat, il est clair qu'on aura beaucoup plus de confiance en cette société d'audit que dans une autocertification, mais que l'autocertification bien évidemment a un aspect coût qui est évidemment beaucoup moindre, alors que l'audit par un tiers est extrêmement coûteux.

Deuxième point qui est important c'est de savoir est-ce qu'on doit développer des standards internationaux ou bien est-ce que cette accréditation devrait se faire suivant des standards qui sont des standards nationaux ou régionaux, et vous voyez tout de suite l'idée: est-ce qu'on ne peut pas développer au niveau européen un standard, un certain nombre de *fair information* practices qui serait compatible avec la protection des données telle qu'elle a été dictée par la directive. Et donc à partir de ce moment-là définir l'appel européen qui pourrait éventuellement être une marque de qualité dans ce qu'on va appeler l'Internet global.

Le point suivant est de savoir: est-ce que la délivrance d'une accréditation est quelque chose de volontaire, est-ce qu'il faut que l'entreprise soit obligée d'agir en sa qualité ou bien est-ce que, au contraire, elle a un caractère volontaire.

Les autres questions m'apparaissent comme aller de soi, en particulier parce qu'il n'est pas évident comment allez-vous sanctionner un site web qui après s'être fait auditer, modifie ses modes d'information, ses modes de pratiques de l'information et à partir de ce moment-là n'est plus en accord avec l'appel qui lui avait été donné au départ.

Toujours en matière d'autorégulation, des réponses à des problèmes qui sont des problèmes plus spécifiques. Le premier problème qu'un certain nombre ont rencontré et qui vient de faire l'objet d'une décision qui a fait beaucoup de bruit aux Etats-Unis, la fameuse décisions Heursling versus Cyber Promotion, c'est le problème du *junk mail*, de l'envoi de mail de manière sauvage, c'est-à-dire de mail non sollicité.

L'idée de la commission de protection des données anglaise c'est de dire: il faudrait pouvoir dans son adresse Internet inscrire le fait que l'on ne souhaite pas de *junk mail* et il faudrait que l'ensemble des sites web ou des sociétés de promotion puissent garantir le respect par eux de cette indication mise par l'internaute lui-même.

Le deuxième c'est en ce qui concerne le problème des robots de recherche, comme Altavista, comme Licos, il faudrait permettre aux personnes de nouveau de faire en sorte que si elles ne souhaitent pas que leur nom puisse faire l'objet d'une recherche, par exemple si je ne désire pas qu'Altavista puisse permettre une recherche par mon nom, bien ses sociétés s'engagent à ne pas permettre de recherches sur base de mon nom. De même, il faudrait lorsque l'on met sur site web soi-même des informations, indiquer que ces informations ne peuvent pas faire l'objet d'une présentation suite à une recherche par un robot de recherche.

Dans la troisième partie, et c'est une partie qui m'importe, je voudrais montrer com-

ment d'une part les directives de protection des données, il y en a deux (la général et la directive Telecom), comment leur interprétation est mise en cause par les pratiques d'Internet. Et je voudrais d'autre part montrer comment si on lit bien ces directives de protection des données, on peut proposer un certain nombre d'exigences aux différents acteurs qui sont sur Internet.

Je prends un premier point qui est un point qui m'apparaît vraiment important. La directive n'est applicable - c'est son scope - qu'à propos de données personnelles, c'est-à-dire des données qui se réfèrent à une personne identifiée ou identifiable.

Lorsqu'on lit cette définition, Double click me dit (et il a raison): je ne traite pas des données personnelles. Pourquoi? Parce qu'en aucune manière je ne sais qui est derrière le navigateur dont j'ai repéré le fonctionnement. Ce que je collecte comme données ce sont des données d'utilisation d'un navigateur X, mais je ne sais pas qui est derrière. Donc il y a un problème, qui est un problème extrêmement important: est-ce que les *cookies* représentent plutôt les données générées par l'envoi des cookies, est-ce que ces cookies représentent des données personnelles. C'est vrai qu'on ne sais pas qui est derrière un cooky, mais on sait, grâce à ce cooky, ce que cette personne fait, même si on ne sait pas qui elle est et qu'à la limite on n'est en aucune manière intéressé.

Premier problème, qui est un problème, me semble-t-il, important d'interprétation de la directive.

Un autre problème: c'est la notion de *processing*, de traitement. Je ne peux pas les voir tous. La directive donne une définition extrêmement large d'une notion de traitement et notamment dit: le traitement peut être chacune des phases de l'utilisation d'une opération: ce peut être la consultation, l'utilisation, la transmission, etc.. Le problème est le suivant: lorsque je ne fais qu'une consultation d'un site web, une visualisation à l'écran, que je ne fais pas de téléchargement, parce que je visualise à l'écran: est-ce qu'il y a processing au sens de l'article 2b? Ça n'est pas évident du tout en ce sens qu'en principe *consultation* est suffisante pour qu'il y ait *processing*. Ça voudrait dire que lorsque je consulte une page web je suis tenu de remplir des fonctions d'information de la personne concernée avec des limites, en principe je suis obligé de faire une *registration* auprès de l'autorité de protection des données, etc.. ce serait, me semble-t-il, aberrant et très peu pratique.

Dernière définition qui me pose des difficultés, là c'est vraiment un problème de fond, c'est le problème de la notion de consentement. C'est un point important parce que, vous le savez, le consentement est une base de légitimité dans le traitement.

En matière d'Internet, grâce à l'interactivité du réseau, je puis chaque fois que je va avoir accès à tel ou tel site, donner mon consentement et le donner à tel ou tel traitement fait par ce site. A partir de ce moment-là les sites web pourraient toujours dire que dans la mesure où l'internaute a marqué son consentement en ce qui concerne les conservations, en ce qui concerne le type d'utilisation, tout est permis. Le consentement peut devenir dans le cas d'un réseau interactif la clé qui ouvre à tout, et on peut, à partir de ce moment-là se poser la question de savoir par exemple: est-ce qu'il est légitime qu'un fournisseur d'accès à Internet garde trace de toutes les utilisations qui sont faites par un de ses clients d'Internet.

Voilà des questions qui sont posées, j'en ai encore bien d'autres. Le problème de l'application de la directive (article 4.1.): on dit de manière extrêmement nette que la directive est applicable si on fait même pour un site web situé à l'étranger, en dehors du territoire de l'Union Européenne, si on fait utilisation de l'équipement situé sur le territoire. Je prends un site web qui est situé aux Etats-Unis et qui est visité par un européen.

Il va de soi que le site web américain pour obtenir des données de l'internaute, données qui sont peut-être nécessaires, va avoir besoin d'un transfert; il va faire utilisation en particulier du navigateur de l'internaute européen, le navigateur de l'internaute européen va lui envoyer des données.

A partir de ce moment-là on pourrait dire, article 41.c: tous les sites web, dans la mesure où ils font utilisation du navigateur de l'internaute européen sont soumis à la directive européenne. C'est une conclusion obtenue récemment dans un rapport qui risque bien évidemment de faire beaucoup de bruit dans la mesure où le destinateur n'est autre que la Commission Européenne.

Je crois aussi que ce serait intéressant de se pencher sur l'application de la directive Telecom. Je prends un exemple, il y en a bien d'autres. Vous savez que l'article 10 mentionne qu'on doit pouvoir s'opposer à un transfert d'appel vers un poste tiers. La directive Telecom dit cela et le dit en pensant au téléphone: est-ce qu'on ne pourrait pas imaginer que ce texte soit également applicable en matière d'Internet? Est-ce qu'on ne pourrait pas imaginer que le fait qu'à un moment donné, étant connecté à un site web, ce site web envoie automatiquement par Interlink - on l'a vu avec Altavista e Double Click - l'ensemble de mes données à un tiers, est-ce que ce n'est pas contraire à l'article 17. Voilà une question, mais il y en a bien d'autres et je vous prie de devoir m'excuser de ne pas avoir le temps de les poser toutes.

Je voudrais arriver à la conclusion: lors d'une réunion qui s'est tenue à Bruxelles, j'étais en face d'un représentant américain qui m'a dit la chose suivante: aux Etats-Unis nous n'avons pas de législation. Vous avez des législations et des autorités de protection de données - celle italienne est exemplaire - mais sont-elles réellement effectives? Nous, aux Etats-Unis, les gens sont réellement sensibles aux problèmes de protection des données et nous avons mis en place des technologies efficaces. Est-ce que ce n'est pas nous, américains, qui avons raison?

Je crois qu'il n'avait en tout cas pas tout à fait tort, en ce sens que nous Européens nous sommes peut-être trop facilement abrités devant des législations ou plutôt derrière des législations et le fait que nous avons des autorités pour dire que tout était très bien et que la protection des données était assurée.

Je crois qu'il faut résolument aller vers une situation où législation et technologie pourront apparaître comme complémentaire. La technologie, elle, ne se développera de façon protectrice des données que s'il y a une pression législative réglementaire, même au-delà d'une pression de la part de la population. Et à cet égard là nous manquons de relais dans le cadre des associations des consommateurs et des associations de libertés civiles.

A l'inverse, les législations ne pourront atteindre leur but, et je le crois très fort, que si elles veulent s'appuyer sur des solutions d'autorégulation et technologiques. Dans ce sens-

là, je crois qu'il y a un rôle et un rôle multiple du secteur public; ce rôle c'est d'abord de mettre dessous pour que l'on trouve des technologies qui soient protectrices des données.

Deuxième rôle - ça va paraître un point important - c'est un rôle de modèle. On a parlé tout à l'heure de l'utilisation d'Internet dans les relations entre administration et citoyens: que l'Etat, dans le cas de ces administrations mette sur pied des procédures modèle de protection des données qui offrent des technologies qui permettent d'assurer cette protection des données.

Le troisième point: rôle de l'état. Un certain nombre de réglementations incitatives. Nous sommes en train de discuter en Belgique sur le fait que les sociétés qui veulent faire du commerce par Internet puissent demander des paiements à l'avance uniquement si elles se sont faites auditées en ce qui concerne le respect des réglementations de protection des consommateurs. Je crois que c'est une manière intéressant de les obliger à autoriser l'autorégulation.

Enfin, dernier point - et j'en termine par là - c'est le fait que l'autorité publique a un rôle de conscientisation et d'éducation du public, depuis l'école me semble-t-il; ce rôle renvoie au fait qu'en définitive la protection des données, elle, sera le fait des internautes eux-mêmes. C'est eux qui grâce l'interactivité du système pourront déterminer, si oui ou non ils acceptent telle pratique, si oui ou non ils acceptent de recevoir le junk mail, si oui ou non ils s'opposent à l'utilisation de leurs données pour telle communication à des fins de marketing ou autre.

Mais ce que je voudrais éviter c'est que on réduise le problème et la problématique de la protection par les internautes eux-mêmes à l'idée que tout va reposer sur une responsabilité individuelle de chaque internaute. Je crois qu'au-delà de la responsabilité individuelle, il existe des solutions dans lesquelles collectivement les internautes doivent pouvoir réclamer des solutions et des solutions y compris de leur régulateur.

Voilà, ce combat est un combat pour nos libertés, et je voudrais vous remercier et en particulier les traducteurs, de votre attention. Merci.

RISERVATEZZA E SICUREZZA DELLE RETI

Prof. Yves Poullet
Faculté Universitaire Notre-Dame de la Paix - Namur

Vorrei innanzitutto ringraziare l'amico Stefano Rodotà e tutti gli organizzatori di questo convegno, per avermi invitato in un luogo il cui prestigio è all'altezza delle sfide di cui la società deve farsi carico quando si parla dei problemi di Internet. Vi ringrazio anche per avere insistito affinché tenessi il mio intervento in francese.

Vorrei prendere in esame tre ordini di problemi. In primo luogo intendo cercare di illustrarvi quali siano i nuovi rischi connessi all'utilizzazione di Internet, i nuovi rischi per quanto riguarda la protezione dei dati. Vorrei quindi tentare un'analisi delle possibili soluzioni. Si è già parlato di PET, le Privacy Enhancing Technologies, e a tale riguardo avrei qualcosa da dire, da specificare, e vorrei anche parlare dei sistemi di autodisciplina esistenti;

infine, cercherò, e questa sarà la terza parte del mio intervento, di analizzare in che modo Internet rimetta in discussione le direttive in materia di protezione dei dati.

Per quanto riguarda i nuovi rischi legati all'utilizzazione di Internet, credo sia sufficiente ricordare le quattro caratteristiche di Internet.

La prima di esse è che Internet è una rete aperta, e ciò significa che chiunque vi si può connettere e, d'altronde, che chiunque vi si può connettere per i fini più svariati - i quali non corrispondono necessariamente agli utilizzi immaginati da chi ha messo certi dati su Internet. In altre parole, è evidente che se tutto il mondo può accedervi, vi saranno problemi di segretezza in rete; se ognuno può utilizzare i dati come meglio crede, ci sarà ad esempio la possibilità, grazie ai motori di ricerca, di individuare senza problemi il profilo di personalità di un soggetto attraverso la sua presenza in un certo numero di gruppi di discussione o attraverso i siti sui quali risulta presente.

Seconda riflessione relativa al carattere aperto della rete: grazie ai legami ipertestuali, è possibile saltare da un sito Web all'altro; ciò comporta un rischio, legato al fatto che tutti i siti Web, come vedremo più avanti, sono interconnessi e possono conservare traccia del percorso effettuato su Internet. Ogni sito può sapere da dove vengo e dove sto andando, e se mi servo di determinati soggetti come fornitori di accesso, questi ultimi possono ricavare un quadro completo del tipo di utilizzo da me effettuato per quanto riguarda Internet.

La seconda caratteristica è rappresentata indubbiamente dal fatto che si tratta di una rete interattiva. Internet pone un nuovo problema, nel senso che io stesso, attraverso l'utilizzazione compiuta dal mio navigatore, genero un certo numero di dati. Sono io a generare dati personali visitando questo o quel sito. Il fatto che in un certo giorno abbia visitato un certo sito e, all'interno di tale sito, una data pagina, ad esempio la pagina sportiva del Washington Post; il fatto che da tale sito sia passato a quello di un'agenzia di viaggi, che mi

sia interessato ai viaggi relativi all'Africa, ecc. ecc.; il fatto che su un sito Web abbia consultato anche le precauzioni necessarie contro l'AIDS...

Un'altra caratteristica è rappresentata senz'altro dal fatto che si tratta di una rete internazionale. Internet non conosce frontiere, e ciò significa che si possono avere paesi nei quali esistono forme di tutela, norme forti in materia di protezione, e altri paesi privi di qualsiasi regolamentazione. Risulta estremamente semplice de-localizzare un sito, e quindi a un certo momento, se un paese prevede norme eccessivamente restrittive, è facile spostare il sito in un altro paese privo di norme di sorta.

Infine, l'ultima caratteristica consiste nel fatto che Internet si caratterizza per la molteplicità degli operatori. Nel quadro di una ricerca che stiamo conducendo per conto della Commissione europea, denominata E-clip, abbiamo cercato di definire una sorta di tipologia degli operatori e delle operazioni compiute, relativamente ad un'attività molto semplice quale l'acquisto di beni su Internet. E vedete, dunque, il numero dei soggetti che possono intervenire: non si tratta soltanto del venditore, ma anche del vettore o dei vettori, che possono essere numerosi, una società di ciber-marketing (ne parleremo più avanti), il fornitore di servizi Internet, la banca; vi si può aggiungere il fornitore di accesso a Internet. Ognuno di questi soggetti ha potuto raccogliere dati in una certa fase della transazione. Abbiamo elencato la tipologia dei dati volta per volta raccolti.

Ecco alcuni dei rischi connessi alle caratteristiche generali di Internet. Vorrei illustrarvi molto rapidamente come, al di là di questi rischi, ne esistano altri derivanti dal fatto che Internet non ha solo un lato visibile, ma ne ha anche uno invisibile: esiste un certo numero di trattamenti che avvengono all'insaputa dell'internauta. Si tratta in primo luogo dei trattamenti che si collocano al livello qualificabile come livello trasporto - il livello basso nell'ambito del modello ISO, ossia il modello di riferimento per quanto riguarda la standardizzazione delle reti di comunicazione.

In questo contesto non mancano i trattamenti invisibili. In primo luogo bisogna considerare che, per quanto riguarda il percorso seguito, non si deve pensare che fra due città vicine come Namur e Bruxelles (abbiamo fatto questo esperimento) il tragitto utilizzato sia quello più breve (60 Km). Il nostro messaggio in partenza da Namur transiterà per il vettore situato in Svizzera, a Ginevra, a Helsinki, a Parigi, ovvero a Washington.

Il secondo rischio è rappresentato dal fatto che, attraverso la manipolazione dei nomi di dominio (il cosiddetto "web spouting"), è possibile fare in modo che il sito Web al quale si accede non sia esattamente il sito al quale si desiderava accedere ma una sorta di sito "trompe l'oeil" - un sito cosiddetto "specchio"; recentemente un sito Web belga è stato oggetto di una perquisizione e di sanzioni penali in quanto aveva creato artificiosamente un sito che riproduceva il sito di un giornale e che evidentemente costituiva un falso ma consentiva di ottenere dati e, in particolare, dati personali.

Il comando ... è una caratteristica della rete che consente di sapere se, ad un dato momento, un altro internauta sia collegato alla rete ed utilizzi la propria connessione; è un modo indiscreto per sapere se si sta utilizzando una versione moderna del telefono.

Questo dunque per quanto riguarda i rischi invisibili legati ai livelli che si possono

definire più bassi.

Per quanto riguarda i livelli più elevati, vi sono altri trattamenti non visibili, come già segnalato, vi sono altri trattamenti possibili e in particolare quelli legati all'esistenza dei cookies. Che cosa sono i cookies? Si tratta semplicemente di briciole di informazioni, ma anche di qualcosa di più, ad esempio può trattarsi di porzioni di programma che vengono inviate al vostro navigatore quando si è connessi ad un certo sito Web e che consentono a tale sito, ogniqualvolta ci si riconnetta ad esso, di riconoscere l'utente. In altri termini, se un giorno mi sono collegato al sito Web del Washington Post e il Washington Post mi ha inviato un cooky, ogni volta che mi riconnetto al Washington Post quest'ultimo potrà sapere che tre giorni, un mese o due mesi prima mi ero già collegato e quali pagine avevo specificamente consultato in quell'occasione.

Lo scopo? È chiaro che gli scopi possono essere ritenuti entro certi limiti legittimi, quando si tratti di garantire la continuità del servizio. Può avvenire che la rete Internet si interrompa, venga a cadere, e allora può essere interessante avere la possibilità di riprendere la transazione dal punto in cui essa si era fermata. Il cooky consente di farlo; il sito Web può riconoscere l'utente e quindi riprendere la transazione dal punto in cui si era interrotta.

Vi sono però scopi meno appropriati, e penso in modo particolare al marketing diretto. Il principio è il seguente: invece di avere un tipo di pubblicità da inviare nello stesso modo a tutta la popolazione, e che non è calibrata su una persona particolare, l'interattività di Internet permette di conoscere con esattezza le preferenze dei singoli utenti e di inviare loro la pubblicità più adatta. Esistono società di ciber-marketing come Double-Click, che ha già oltre 2500 società affiliate (e si tratta di una cifra destinata verosimilmente a crescere), che raccolgono i dati di utilizzo di Internet a partire da alcuni siti che sono affiliati a tali società, dopo di che sono in grado, sulla base di questa raccolta estesa, di calibrare più precisamente le preferenze dei singoli internauti.

Se me lo consentite, vi illustro rapidamente il funzionamento di questi sistemi quando mi connetto ad un sito Web, ad esempio al sito di Altavista; è un esperimento che abbiamo compiuto più volte, e funziona molto bene - o molto male, a seconda dei punti di vista.

Quando mi connetto al sito di Altavista per effettuare una ricerca relativa ad un nome o eventualmente ad un termine, Altavista ha un legame ipertestuale (automatico) con Double-Click; ciò significa che quando mi connetto ad Altavista, la società di marketing mi invia automaticamente un cooky e riceve automaticamente un certo numero di informazioni. Si tratta in prima istanza di informazioni che comunque andrebbero inserite nell'intestazione del messaggio: la pagina che sto per visitare, il fatto che eventualmente è già stato inviato un cooky al mio navigatore, il fatto che utilizzo un certo tipo di navigatore (Netscape, e quale versione), e che lo utilizzo su un sistema operativo di una data generazione, e infine l'indirizzo dell'internauta. Quest'ultimo indirizzo non è stabile, non è fisso, e quindi si può ritenere che non si tratti di un dato personale; tuttavia, il problema riguarda le informazioni generate dal cooky, in quanto con tale cooky la società di marketing e Altavista potranno sapere non già chi sono, perché non sapremo mai chi è l'utente dietro al navigatore, bensì, e con certezza, cosa fa questo determinato utente.

Questo desideravo illustrarvi per quanto riguarda le modalità di funzionamento delle società di ciber-marketing, che a mio giudizio rappresentano un grave problema.

A conclusione di queste considerazioni sui trattamenti invisibili, vorrei aggiungere che esiste una differenza, ed una differenza netta, fra quello che l'internauta crede di fare e quello che avviene in realtà.

Che impressione si ha collegandosi a siti Web? L'impressione è che ciascuno di tali siti sia qualcosa di autonomo, che non esistano interrelazioni fra i siti. Quando ci si collega ad Altavista, sembra di uscire da Altavista e di andare in un sito 1, quindi in un sito 2, poi in un sito 3, e così via; la realtà è invece ben diversa.

Tre considerazioni si impongono a tale proposito. Primo: tutti i siti che visitiamo sono interconnessi, ossia ogni sito visitato conserva traccia del sito da noi visitato in precedenza e, ovviamente, una traccia del sito verso il quale ci spostiamo. Si tratta di un primo dato personale che può risultare interessante: tizio viene dalla pagina x, le Trois Suisses, e va alla pagina y, per esempio la Gazzetta dello Sport.

Secondo: nella misura in cui questi siti sono affiliati ad una NTTP, ad esempio una società di ciber-marketing. Perché NTTP? Ho voluto fare un piccolo gioco di parole: NTTP sta per Not-Trusted-Third-Party, ossia si tratta di un terzo non fidato che raccoglie informazioni a nostra insaputa. Bene, questo soggetto, nella misura in cui è collegato ad Altavista e al sito 1, può sapere ogni volta che tipo di utilizzazione viene compiuta del sito in questione.

Tutto ciò è lecito, e la mia impressione è che non si sia riflettuto abbastanza su questo punto: si parla molto di regolamentazione dei fornitori di accesso, si parla di regolamentare i fornitori di accesso Internet, ma non si considera con pari attenzione il fatto che chi permette tutto ciò è evidentemente il navigatore, il fatto che il navigatore consente l'invio del cooky, fa in modo che, automaticamente, per il solo fatto di utilizzare il nostro browser, siano possibili modalità di utilizzazione dei dati che mi sembrano quanto meno sleali.

Ora che abbiamo esaminato i rischi, vorrei riflettere insieme a voi su alcune soluzioni alle quali si può ricorrere per evitare tali rischi. Ma, prima di analizzare queste soluzioni, le soluzioni tecniche, autoregolamentative e legali, vorrei porvi tre domande che mi sembrano fondamentali. Per ciascuna soluzione mi sembra che ci si debbano porre tre domande.

Prima domanda: riguarda la legittimità della soluzione proposta. Legittimità nel senso di sapere se chi propone una determinata soluzione sia legittimamente autorizzato a proporla; il che non significa necessariamente che debba trattarsi di un soggetto designato in un'ottica costituzionale, ma di certo non vuol neppure dire che la legittimità implichi una discussione aperta che consenta di prendere in esame il punto di vista anche dei diretti interessati (gli internauti), e in tal senso ci si può interrogare sulla legittimità di alcune soluzioni di autoregolamentazione.

Secondo punto che mi sembra importante: il fatto che la soluzione deve essere conforme, e la conformità consiste, a mio giudizio, nella necessità che si abbia *compliance*, che si tratti di una soluzione adeguata ai principi in materia di protezione dei dati - una volta che questi ultimi siano stati definiti.

Infine, l'autoregolamentazione è un'illusione ottica se non è efficace. E per appurare se sia efficace occorre verificare se l'autorità che deve applicare l'autoregolamentazione, o eventualmente i terzi incaricati del rispetto della regolamentazione, dispongono degli strumenti necessari, se hanno la possibilità di imporre sanzioni e che tipo di sanzioni.

Fra le diverse soluzioni, la prima è quella di cui parla tutto il mondo, è senz'altro la soluzione tecnica. Mi riferisco alla definizione di Herbert: di fatto si tratta di costruzioni, di strumenti tecnici che fanno in modo che si tenti di minimizzare o di evitare del tutto che si abbiano trattamenti di dati personali.

Che cosa è già disponibile da tale punto di vista? La PET è stata definita da George Heidelberg, in un articolo che ha fatto molto rumore sull'altra riva dell'Atlantico, la *lex informatica*, che a giudizio dell'autore presentava un certo numero di vantaggi rispetto alla lex classica. Vanno distinti due livelli per quanto riguarda la PET. In primo luogo, un certo numero di tecniche finalizzate a consentire la protezione dei dati si collocano al livello dell'anonimato e della segretezza del messaggio. Si tratta di fare in modo che chiunque possa inviare un messaggio in modo anonimo e che tale messaggio circoli con sicurezza. La prima PET è rappresentata evidentemente dall'utilizzo di tecniche di cifratura. Vi ricordo che il Working Group di Berlino che si occupa di privacy nel settore delle telecomunicazioni aveva raccomandato fin dal 1995, quando era iniziato il dibattito relativo alla cifratura, di offrire la possibilità di utilizzare liberamente tecniche di cifratura in modo da evitare ogni rischio per la segretezza dei messaggi.

Un secondo tipo di servizi è esemplificato dalla M... finlandese, che offriva servizi di anonimizzazione - ossia servizi di corrispondenza anonima che servono esclusivamente a fare in modo che il sito web o il vostro corrispondente non possa sapere chi è il mittente del messaggio; in sostanza, chi scrive passa per un terzo, essendogli attribuito un indirizzo *just in case* - un indirizzo che permetterà ovviamente di non essere riconosciuti dalla persona cui si invia il messaggio. Si tratta di un sistema con cui si fornisce all'interessato una sorta di maschera di identità.

L'ultima possibilità è rappresentata dal cosiddetto surfing anonimo. L'idea del surfing anonimo sta prendendo sempre più piede. Durante l'ultima riunione del gruppo di Berlino sono state compiute due riflessioni. Primo punto: l'affermazione che i browser, i navigatori di Netscape, il vostro Microsoft Explorer, devono consentire la navigazione in forma anonima; sarebbe una conquista straordinaria, quella di non rivelare la propria identità. E la seconda raccomandazione che mi sembra importante riguarda la possibilità per tutti di utilizzare pseudonimi. Penso che sia un punto fondamentale quello di non dover firmare con il proprio nome, di persona identificata, bensì di poter firmare utilizzando la copertura di uno pseudonimo. Sono due raccomandazioni che dovranno senz'altro trovare applicazione.

Quando si parla di PET si pensa ovviamente in primo luogo agli sviluppi più recenti, in termini di riflessione, ma anche in termini di applicazioni tecnologiche, riflessioni attuali che si riferiscono alla *piattaforma per le preferenze* in tema di privacy. L'idea è la seguente: si tratta di dare attuazione, nel settore della privacy, alle soluzioni richiamate questa mattina, le soluzioni menzionate in tema di messaggi osceni o pornografici. L'idea è di dire: utilizzia-

mo il sistema PICS - *platform for Internet content selection* - ma utilizziamolo in modo da consentire la tutela della privacy e non soltanto la protezione nei confronti dei messaggi osceni o di altra natura.

Queste tecnologie sono state messe a punto dal Worldwide Web Consortium; come potete vedere, esso comprende interlocutori americani, francesi, giapponesi - in sostanza, tutte le società, Microsoft, Netscape, IBM, Compaq, ma anche Double-click, i grandi server, sono presenti in questo consorzio e partecipano alla sua attività.

L'idea è la seguente, la riassumo in rapporto a quattro soggetti. Il primo soggetto è l'organo di etichettatura, che deve specificare a priori il contenuto delle etichette e il loro significato. Se affermo che una società rispetta i principi di protezione dei dati, che cosa significa? In prima istanza, si tratta di sapere che cosa si intenda per dato personale. E cosa significa ciò in termini di utilizzo legittimo di tale dato? Quella certa società rispetta i principi di protezione perché utilizza i dati per sé, perché li utilizza eventualmente per esclusivi scopi di tariffazione, ovvero perché anche se li comunica, permette ai terzi di esercitare il diritto di accesso?

La prima richiesta da fare all'organo di etichettatura è la seguente : individuate una terminologia che consenta a priori di sapere che, quando si afferma che un certo sito web offre una protezione di tipo 2, bene, che si sappia cosa significa questa protezione di tipo 2 in termini di conservazione dei dati, di natura dell'utilizzo, in termini ovviamente di diritto di accesso.

In primo luogo occorre mettere a punto un vocabolario comune, e vi assicuro che è un punto estremamente delicato, estremamente difficile; la Commissione francese ha elaborato in merito una serie di riflessioni preliminari sul vocabolario utilizzato dalla P3P.

Seconda idea: fare in modo che si possa conoscere la situazione dell'etichetta. Che cosa vuol dire etichetta in materia di protezione dati? Che cosa vuol dire "etichetta 2" in materia di protezione dati? ecc. ecc. Occorre garantire la massima diffusione.

Il secondo soggetto - e si tratta ovviamente del soggetto più delicato: una volta definito il vocabolario di cui sopra, chi deve vigilare sul sito web e stabilire che un certo tipo di sito corrisponde all'etichetta di tipo 1, 2 o 3. Può trattarsi del sito web stesso, nel qual caso si parla di self-rating, oppure può trattarsi di un soggetto terzo, ad esempio di una società di auditing che agisca per conto del sito web.

Una volta definita l'etichetta, deve essere resa pubblica. Un certo sito web ha un'etichetta di tipo 1, 2, 3...

Cos'altro resta da fare? Resta da chiarire il ruolo di quella che può essere indicata come la società di software, e in particolare il ruolo delle società che sviluppano i programmi di navigazione. Queste ultime devono permettere, credo, due cose. In primo luogo, che il programma di navigazione sia configurato in modo da consentire all'internauta di esprimere la specifica preferenza - ossia, di dire "Per quanto mi riguarda, voglio assolutamente un livello di protezione dei dati di tipo 7, il livello più elevato".

E poi, secondo punto: una volta che abbia configurato il mio programma di navigazione con l'etichetta di tipo 7, occorre evidentemente che il mio programma possa, quando incontra un sito web che non accetti un livello di protezione di tipo 7 o che offra semplicemente un livello di protezione inferiore, bene, che possa bloccare l'accesso a tale sito.

Ovvero, e ciò rappresenta chiaramente un grosso progresso rispetto alla tecnologia X iniziale, ovvero che possa offrire all'internauta che si rende conto del fatto che il sito web al quale intende connettersi non possiede il livello di protezione desiderato a priori, la possibilità di dare inizio eventualmente ad un negoziato. Come dire: voi non mi garantite quella data protezione, io chiedo di avere questa protezione, che cosa mi offrite a titolo di garanzia supplementare?

Ecco quello che l'internauta, il quarto soggetto in causa, deve poter fare: se il sito web garantisce lo stesso livello di protezione, non c'è problema, si ha quello che si chiama *automatic matching,* ma se invece non viene garantito lo stesso livello, allora interviene la trattativa negoziale.

Ci sarebbero ancora molte cose da dire, ma non voglio indugiare su un punto sul quale potremo tornare più avanti - ossia, il problema della regolamentazione dei navigatori; su questo punto il nostro gruppo di ricerca ha elaborato un certo numero di raccomandazioni, che sono state presentate alla conferenza europea delle autorità di protezione dei dati. Potremo tornare su questo punto quando lo desiderate.

Per quanto riguarda l'autoregolamentazione: l'idea va vista nel contesto di un sistema di normalizzazione. Non si potrebbero definire a priori modalità di gestione di dati personali che siano conformi ai principi in materia di protezione dati. L'autodisciplina, e in questo senso è necessario distinguerla dalle PETs, pone maggiormente l'accento sulle modalità di gestione, mentre le PETs pongono evidentemente l'accento su tecnologie che, a priori, vietano l'una o l'altra modalità di gestione. Nel quadro dell'approccio ISO, il principio chiarissimo è di dire: cercheremo di definire modalità di gestione dell'informazione, all'interno delle imprese che offrono servizi via Internet, che possano essere conformi ad una serie di principi in materia di protezione dei dati.

Si tratta di un'attività cui ha dato inizio nell'ambito dell'ISO il *Consumer Policy Committee*, ma è interessante osservare la tipologia dei consumatori che si sono mostrati interessati a questo sistema e che per primi ne sono stati coinvolti.

È un sistema che ovviamente si basa su un certo numero di procedure, in quanto il problema consiste nel poter dire, una volta definito un elenco di pratiche in materia di utilizzo corretto dell'informazione, che un certo sito web si conforma allo standard definito una volta per tutte. Pertanto, il problema che si pone è come regolare la questione delle procedure di certificazione dei cittadini; come fare perché sia riconosciuta la conformità di un sito web.

Primo quesito: stiamo collaborando con società di revisione per tentare di individuare un approccio possibile. Il primo quesito sottopostoci è il seguente: la certificazione, e si tratta un po' dello stesso problema relativo alla P3P, viene compiuta dal sito web stesso, anche se deve essere effettuata necessariamente da un soggetto terzo abilitato a verificare il funzionamento dell'impresa. Si tratta di un problema di estrema delicatezza; è evidente che si avrà molta più fiducia in questa società di revisione rispetto ad un'autocertificazione, ma è chiaro d'altra parte che l'autocertificazione presenta una componente costi molto minore, mentre il processo di revisione da parte di un terzo risulta estremamente costoso.

Secondo punto importante: sapere se occorre definire standard internazionali oppure se la certificazione debba avvenire secondo standard che possono essere standard nazionali o regionali, ed ecco immediatamente il concetto: se non si possa elaborare a livello europeo uno standard, un certo numero di *fair information practices* che siano compatibili con la protezione dei dati così come prevista dalla direttiva. E, a partire da tale momento, definire il marchio europeo che potrebbe essere eventualmente un marchio di qualità entro il cosiddetto Internet globale.

Il punto successivo da chiarire è il seguente: se la certificazione sia qualcosa di volontario, se l'impresa debba essere obbligata ad attivarsi in quanto tale, ovvero se appunto sia un adempimento volontario.

Gli altri quesiti mi sembrano di facile risposta, in particolare perché non è chiaro come si possa sanzionare un sito web che, dopo essersi sottoposto ad un controllo esterno, modifichi le pratiche informazionali, e cessi quindi di essere conforme all'etichetta assegnata inizialmente.

Sempre in materia di autoregolamentazione, alcune risposte a problemi di natura maggiormente specifica. Il primo, che molti avranno incontrato e che è stato oggetto di una sentenza che ha fatto molto rumore negli USA, la famosa sentenza nel caso Heursling v. Cyber Promotion, è il problema del junk mail, ossia l'invio indiscriminato di corrispondenza, corrispondenza quindi indesiderata.

L'idea dell'autorità inglese di protezione dati è quella di dire: sarebbe opportuno che, al proprio indirizzo Internet, ciascuno potesse indicare che non desidera ricevere junk mail, e sarebbe opportuno che tutti i siti web o le società di promozione possano garantire il rispetto di tale indicazione inserita dallo stesso internauta.

Il secondo riguarda il problema dei motori di ricerca, come Altavista, come Lycos; si dovrebbe consentire ai singoli, ancora una volta, di far sì che, se non desiderano che il loro nome sia oggetto di una ricerca, ad esempio se io non desidero che Altavista permetta l'effettuazione di una ricerca basata sul mio nome, bene, che tali società si impegnino a non consentire ricerche in base al mio nome. Allo stesso modo, qualora si pubblichino autonomamente informazioni sul sito web, sarebbe opportuno indicare che tali informazioni non possono essere oggetto di una descrizione successiva ad una ricerca effettuata attraverso un motore di ricerca.

In terzo luogo, e si tratta di un punto di particolare interesse per quanto mi riguarda, vorrei illustravi come da un lato le direttive in materia di protezione dei dati (ne esistono due, quella generale e la direttiva sulle telecomunicazioni), come la loro interpretazione sia messa in discussione dalle prassi comunemente seguite su Internet. E vorrei inoltre illustrarvi come, se si leggono con attenzione tali direttive, si possano proporre un certo numero di requisiti ai vari soggetti che agiscono su Internet.

Parto da una prima considerazione che mi sembra veramente fondamentale. La direttiva si applica - si tratta dell'ambito specifico - esclusivamente ai dati personali: ossia, ai dati che si riferiscono ad una persona identificata o identificabile.

Dinanzi a tale definizione, Double-Click mi dice (ed ha ragione): io non tratto dati

personali. Per quale motivo? Perché non so assolutamente chi vi sia dietro il navigatore di cui ho individuato il funzionamento. I dati che raccolgo sono dati di utilizzo di un navigatore X, ma non so chi vi si nasconda dietro. Esiste dunque un problema, un problema di estrema importanza: se i cookies rappresentino i dati generati dall'invio dei cookies stessi, o non piuttosto dati personali. È vero che non si sa chi si nasconda dietro ad un cooky, ma grazie al cooky è possibile sapere cosa fa questa determinata persona, pur ignorandone l'identità - il che, al limite, non riveste alcun interesse. Primo problema, e si tratta, a mio giudizio, di un problema importante in termini di interpretazione della direttiva.

Altro problema: si tratta del concetto di *processing*, di trattamento. Non posso prevedere ogni eventualità. La direttiva dà una definizione assai ampia di un concetto di trattamento, e in particolare afferma che per trattamento si intende ogni fase di utilizzo di un'operazione: ad esempio, la consultazione, l'utilizzazione, la trasmissione. ecc. . Il problema che si pone è il seguente: se mi limito a consultare un sito web, visualizzandone il contenuto sul monitor, nel qual caso non si ha alcuno scaricamento di dati in quanto li visualizzo esclusivamente sul monitor, si può parlare di trattamento ai sensi dell'articolo 2(b) della direttiva?

Non è un quesito di immediata risoluzione, in quanto in linea di principio la consultazione è sufficiente a configurare un "trattamento". Ciò significherebbe che, quando si consulta una pagina web, si è tenuti ad adempiere ad alcuni obblighi di informazione nei confronti dell'interessato e al rispetto di alcune limitazioni; in linea di principio, si sarebbe tenuti ad effettuare una notificazione presso l'autorità responsabile per la protezione dei dati, ecc., il che mi sembra un'aberrazione oltre che assai poco pratico.

Ultima definizione che mi comporta alcune difficoltà: si tratta effettivamente di un problema di fondo, relativo al concetto di consenso. È un punto importante, poiché come sapete il consenso rappresenta un fondamento di legittimità ai fini del trattamento. In ambito Internet, grazie all'interattività della rete, è possibile dare il proprio consenso ogniqualvolta si desidera accedere a un determinato sito, e acconsentire ad un determinato trattamento effettuato da tale sito. A partire da questo momento i siti web potranno sempre affermare che, nella misura in cui l'internauta abbia indicato il proprio consenso per quanto riguarda la conservazione o il tipo di utilizzo, tutto è permesso. Il consenso può divenire, nel caso di una rete interattiva, la chiave che apre tutte le porte, e a questo punto si tratta di stabilire, ad esempio, se sia legittimo che un fornitore di accesso a Internet conservi traccia di tutti gli utilizzi compiuti da uno dei propri clienti Internet.

Queste sono solo alcune delle problematiche da prendere in esame, ve ne sono molte altre. Il problema dell'applicazione della direttiva (articolo 4.1.): si afferma in modo estremamente netto che la direttiva trova applicazione qualora si utilizzino apparecchiature situate sul territorio europeo, anche per conto di un sito web situato all'estero, al di fuori del territorio dell'Unione Europea. Consideriamo il caso di un sito web situato negli USA e visitato da un cittadino europeo.

Va da sé che il sito web americano avrà bisogno di un trasferimento di dati per raccogliere dati dell'internauta, dati che sono magari necessari; in particolare, dovrà utilizzare il programma di navigazione dell'internauta europeo, che dovrà inviargli i dati eventualmente

richiesti. A questo punto si potrebbe dire, articolo 4.1(c): tutti i siti web, nella misura in cui utilizzano il programma di navigazione dell'internauta europeo, sono soggetti all'applicazione della direttiva europea. È una conclusione cui giunge un recente rapporto che rischia evidentemente di fare molto rumore, essendo destinato né più e né meno che alla Commissione europea.

Credo inoltre che sarebbe interessante esaminare l'applicazione della direttiva sulle telecomunicazioni. Farò un esempio, ma ve ne sono molti altri. Sapete che l'articolo 10 afferma che deve esistere la possibilità di opporsi al trasferimento di chiamata a terzi. La direttiva afferma tale diritto pensando al telefono: non si potrebbe immaginare che la disposizione si applichi egualmente anche ad Internet? Non si potrebbe immaginare che, per il fatto che a un dato momento, essendo collegati ad un sito web, tale sito web invii automaticamente via Interlink (l'abbiamo visto nel caso di Altavista e DoubleClick) tutti i miei dati ad un terzo, ciò risulti contrario all'articolo 17? Questo è uno dei dubbi possibili, ma ve ne sono molti altri, e vi prego di scusarmi per non avere il tempo di illustrarli tutti.

Vorrei arrivare alle conclusioni. Durante una riunione tenutasi a Bruxelles, mi trovavo seduto dinanzi ad un rappresentante americano che mi ha detto quanto segue: negli USA non abbiamo legislazione. Voi avete leggi e autorità competenti in materia di protezione dei dati - quella italiana è esemplare da tale punto di vista -, ma sono realmente efficaci? Noi, negli USA, siamo effettivamente sensibili al problema della protezione dati, e abbiamo messo a punto tecnologie efficaci. Non è che magari siamo noi americani ad avere ragione?

Penso che il mio interlocutore non avesse comunque del tutto torto, nel senso che noi europei tendiamo forse con troppa facilità a farci scudo della legislazione (o meglio, a nasconderci dietro il fatto che esiste una legislazione) e dell'esistenza di autorità competenti per affermare che tutto va perfettamente e che abbiamo assicurato la protezione dei dati.

Credo che si debba andare risolutamente verso una situazione in cui legislazione e tecnologia possano risultare complementari. La tecnologia non potrà evolvere in modo da tutelare i dati se non esiste una pressione legislativa di natura regolamentativa, anche al di là della pressione esercitata da parte dell'opinione pubblica. E, a tale riguardo, mancano collegamenti fra le associazioni dei consumatori e le associazioni per le libertà civili.

Per contro, la legislazione non potrà raggiungere gli obiettivi che si prefigge, e ne sono profondamente convinto, se non accetta di integrarsi con soluzioni di natura autoregolamentativa e tecnologica. In tal senso credo che il settore pubblico abbia un ruolo da svolgere, ed un ruolo dalle molteplici sfaccettature: si tratta di mettere rapidamente in atto questo ruolo per individuare risposte tecnologiche in grado di assicurare la protezione dei dati.

Terzo punto: ruolo dello Stato. Un certo numero di norme che servano da incitamento. In Belgio stiamo dibattendo sul fatto che le società che desiderano commerciare via Internet possano chiedere pagamenti anticipati solo se abbiano accettato di sottoporsi ad un controllo esterno per quanto riguarda il rispetto delle norme a tutela dei consumatori. Mi sembra un modo interessante di obbligare questi soggetti a consentire l'autoregolamentazione.

Infine, ultimo punto, e qui termino il mio intervento, il fatto che l'autorità pubblica

deve svolgere un ruolo di sensibilizzazione e di educazione del pubblico, direi fin dalla scuola; tale ruolo rinvia al fatto che, in ultima analisi, la protezione dei dati spetta agli internauti stessi. Sono questi ultimi che, grazie all'interattività del sistema, potranno stabilire se accettare o meno una determinata prassi, se accettare o meno di ricevere junk mail, se opporsi o meno all'utilizzo dei propri dati per una determinata comunicazione a fini di marketing o di altra natura.

Tuttavia, quello che vorrei evitare è di ridurre il problema e la problematica della protezione da parte degli stessi internauti al concetto che tutto si basi sulla responsabilità individuale dei singoli internauti. Credo che, al di là della responsabilità individuale, esistano soluzioni nel cui ambito gli internauti devono poter chiedere collettivamente la definizione di soluzioni, anche da parte dei rispettivi organi normativi.

Stiamo lottando per le nostre libertà. Vi ringrazio per l'attenzione, e ringrazio in modo particolare gli interpreti. Grazie.

INTERVENTI

Prof. Giampio Bracchi

Alcune considerazioni per ricondurre le interessanti considerazioni che sono state proposte nei precedenti interventi nella realtà delle aziende e delle pubbliche amministrazioni italiane. Vorrei cercare di offrire, sulla base dei risultati di alcuni osservatori sull'utilizzo delle tecnologie dell'informazione nelle principali imprese e pubbliche amministrazioni italiane, che il Politecnico di Milano gestisce da alcuni anni, una visione di quella che è la realtà dell'utilizzo di Internet negli ambienti sia privati che pubblici.

Sappiamo tutti che in Europa in generale, e specificamente in Italia, denunciamo alcuni ritardi nella penetrazione della tecnologia dell'informazione nella società e nel mondo economico in particolare. Molti di questi dati sono ben conosciuti. Sappiamo che la spesa informatica in Italia è solo un terzo rispetto a quella negli Stati Uniti in percentuale del prodotto interno, mentre in Europa è poco più della metà, e sappiamo anche che il numero di personal installati ogni 100 persone in Italia è un quarto rispetto agli Stati Uniti. Il numero di web servers ancora una volta denota un differenziale consistente: 40 per 1000 abitanti negli Stati Uniti, 11 in Europa, 4 in Italia. E solo nella telefonia radiomobile che l'Italia e l'Europa sono allineati coi valori nordamericani, ma anche in Europa ci sono differenze sostanziose.

Ad esempio, nel mercato delle famiglie e dei piccoli affari, la penetrazione dei personal computers in Italia è del 40% inferiore rispetto al Regno Unito, che viene di solito assunto come punto di riferimento nell'uso dei servizi telematici, perché essi prima sono stati colà sviluppati, prima sono stati liberalizzati, e quindi c'è una maggiore intensità di uso.

Se noi guardiamo, rispetto alle famiglie che hanno personal computer, quanti hanno l'abbonamento a Internet, vediamo che il rapporto è 1 a 4 tra l'Italia e il Regno Unito. Il che vuol dire che nelle famiglie italiane c'è un sesto degli abbonamenti a Internet del Regno Unito. Questo ci dice come, nel nostro Paese, l'accento in questi anni debba essere soprattutto sulla promozione dell'uso delle reti pur nell'ambito delle regole.

Come si collocano nell'automazione le aziende italiane? Esse, rispetto all'Europa, sono partite un po' in ritardo nell'automazione, anche a causa della struttura fatta di piccole imprese, da sempre impegnate più in iniziative di inseguimento che in iniziative pionieristiche, però l'Italia, fino alla fine degli anni ottanta, presentava ritmi di crescita negli investimenti informatici superiori rispetto agli altri Paesi europei, stava cioè recuperando il ritardo.

Questo non è più vero a partire dal '93-94, né nelle aziende né nella pubblica amministrazione; in effetti si rileva che la crescita italiana prevista per il '98 nella spesa per tecno-

logia dell'informazione è inferiore a quella di molti Paesi europei, anche di Paesi che stanno recuperando il ritardo come la Spagna.

Dobbiamo concludere che in Italia c'è più un accento sulla riduzione dei costi che sulla utilizzazione della tecnologia come fattore di sviluppo. Questa è una situazione degli ultimi 4-5 anni, che deve fare riflettere perchè non si recupera più il ritardo che esisteva.

Dati più positivi vengono dall'uso delle telecomunicazioni. Gli investimenti delle aziende italiane in telecomunicazioni crescono a ritmi pari a circa il doppio rispetto a quella degli investimenti informatici: investimenti informatici più 7% all'anno di crescita media, telecomunicazioni più 16%. Però l'andamento ha accelerato a partire dal '96. Negli ultimi due anni, in effetti, le aziende italiane iniziano in modo significativo a investire in tecnologie di comunicazione, con una crescita di quasi il 30% all'anno.

Questa crescita è superiore, per le telecomunicazioni, ai dati europei. Chiaramente non è solo questione di investimenti, è anche questione dell'abbattimento di costi unitari di telecomunicazione, ma c'è indubbiamente un atteggiamento differente.

Questa spesa per telecomunicazioni è dedicata quasi interamente a quelli che si chiamano i servizi "legacy", ai vecchi sistemi su mainframe collegati con reti di trasmissione dati, quelli che sono largamente diffusi, ad esempio nell'amministrazione centrale dello Stato.

La parte delle spese di comunicazione dedicata a Internet è molto bassa, nel '96 è stata pari al 4%, con una crescita però nel '97 rispetto al '96 del 595%. Questo vuol dire che la realtà Internet nelle aziende costituisce ancora un qualche cosa di molto embrionale (il 4% della spesa totale di comunicazioni), con una sestuplicazione, però, nel giro di un anno, il che vuol dire che le aziende iniziano a usare seriamente Internet e quindi si porranno anche i problemi di protezione della privatezza con Internet.

Nelle aziende leader italiane industriali e di servizi, l'accesso a Internet da tutte le postazioni aziendali avviene solo nel 40% dei casi, quindi si può affermare che esso non è ancora diffuso a livello dell'azienda, ma è limitato a un sottoinsieme delle posizioni di lavoro esistenti in azienda.

Per quanto riguarda la presenza di un sito aziendale con pagine Internet, esso è già presente nell'80% dei casi, però lo scopo normalmente non è quello di fare commercio elettronico, ma è soprattutto quello di illustrare i prodotti dell'azienda, di avere della pagine informative. In una caratteristica le aziende italiane presentano valori molto elevati rispetto al contesto internazionale, quella del numero di pagine per ogni sito web: i siti web delle aziende italiane sono, infatti, particolarmente voluminosi come numero di pagine. Questo vuol dire che il sito web è qualcosa di informativo, non è qualcosa che si rivolge in modo snello alla clientela.

Infine, per completare l'analisi sulle aziende, si può richiamare un confronto internazionale sull'uso di Intranet (le tecniche Internet per colloquiare dentro l'azienda), e di Extranet (per colloquiare dall'azienda con i clienti e con i fornitori); vediamo che nel nostro osservatorio il 40% delle aziende sta ricercando una soluzione ma non l'ha ancora attuata, mentre, se andiamo a esaminare il riferimento nordamericano, vediamo che nel 39% dei

casi Intranet è già in esercizio. Nel '96, dunque, anche le aziende italiane sono partite sulla strada dell'uso di Internet al proprio interno (l'Intranet) e per offrire servizi ai propri clienti (l'Extranet), ma accumulano un ritardo di un paio di anni rispetto alle aziende nordamericane, che su questa strada si trovano già abbastanza più avanti. Il mercato italiano si è, però, ormai avviato, e occorre quindi avere delle attenzioni sul modo con cui si sviluppa l'utilizzo di Internet. L'accento deve naturalmente essere sull'aiutare lo sviluppo con dei cantieri di lavoro, con delle promozioni in certi settori di attività.

Ma più interessante, ai fini soprattutto di questo convegno, è la realtà della pubblica amministrazione, proprio perché la pubblica amministrazione contiene molti dati che riguardano le persone, molti dati sensibili. Se pensiamo al settore della sanità questo è del tutto evidente, ma anche il settore del fisco o il settore della previdenza, ad esempio, hanno caratteristiche simili.

Cominciamo dai comuni italiani, usando i risultati di un osservatorio del Politecnico di Milano che effettua il monitoraggio della realtà informatica dei comuni italiani leader.

Nel '97 ormai il 60% dei comuni italiani aveva accesso a Internet. I comuni cioè, hanno qualche posizione di lavoro da cui accedono a Internet.

Più interessante è vedere come si utilizzano le reti civiche, con cui i comuni non solo effettuano l'accesso a Internet, ma instaurano una comunicazione a volte monodirezionale (nei due terzi dei casi), ma spesso anche bidirezionale, per un colloquio su vari argomenti con i cittadini, per creare gruppi di discussione, per dare accesso ai documenti della pubblica amministrazione, per ricevere commenti e così via. Le città in rete Internet in Europa, al settembre '97 erano un centinaio in Italia, un valore non molto differente dagli altri Paesi. In Germania a quel momento erano 400, in Olanda (piccolo Paese però evoluto su questa strada) 139, ma il Regno Unito era nella situazione dell'Italia e la Francia o la Spagna stavano dietro.

Un particolare curioso è che un terzo di queste città sono nel centro Italia, che, almeno nell'uso delle reti civiche, ha finora dimostrato una maggiore dinamicità.

Che cosa fanno queste reti civiche? Questo diventa un discorso interessante anche agli effetti del nostro convegno. Da queste reti civiche si va sulle banche dati che in qualche modo sono collegate al comune, soprattutto sulle banche dati delle aziende municipalizzate, della provincia, delle università, delle ASL, di altri enti, mentre le banche dati comunali collegate alla rete civica sono soprattutto l'Anagrafe, gli archivi delle municipalizzate, delle USL, l'archivio delle delibere, l'archivio dei tributi. In definitiva, in molti casi si accede ad alcune informazioni che dovrebbero essere nella più ampia trasparenza (il D.L. 241 vorrebbe che le delibere fossero disponibili per tutti, non c'è da proteggerle ma c'è da verificare che non si riesca a identificare l'individuo che ha accesso a queste cose), ma in altri casi ci si deve invece preoccupare di impedire che a dati sensibili, che in qualche modo sono recuperabili nella banche dati pubbliche, possano avere accesso persone non autorizzate.

Vedendo che da Internet si va sulle altre banche dati, in particolare quelle delle USL, nasce il problema degli strumenti di protezione del mondo Internet verso le banche dati.

Nelle aziende private questo problema è meno accentuato, perché le banche dati non sono sensibili, o meglio sono sensibili agli effetti dell'azienda che non vuole che dall'esterno

si possa andare sui propri archivi, ma non per ragioni legate a un interesse collettivo, bensì per una ragione legata alla protezione di una proprietà dell'azienda stessa.

Nel caso delle banche dati pubbliche, viceversa, esiste un interesse collettivo, è in questo caso che i vari fire-wall entrano in gioco. Non si possono fare progetti di interconnessione delle reti pubbliche Internet con le banche dati della pubblica amministrazione sensibili, senza attivare adeguate protezioni verso l'accesso a queste banche dati. Abbiamo ascoltato prima una relazione sugli strumenti tecnici, i vari fire-wall che ci consentono di proteggere questo accesso. Ma spesso si affronta il problema con un po' di superficialità, senza queste attenzioni, si cerca di fare, ma non ci si preoccupa di vedere come si deve fare in modo che tutto sia protetto.

Questo ci porta verso il concetto della pubblica amministrazione estesa, proprio perché le reti ci portano ad avere una pubblica amministrazione allargata, dove i dati stanno dove devono stare, e senza il bisogno di centralizzarli tutti; questa è una possibilità importante, perché nel passato, per avere una interoperabilità delle banche dati, bisognava collocarle tutte nello stesso sito. Molti ricorderanno 20 anni fa, gli esempi della "data centralen" che esistevano nei Paesi nordeuropei, e i problemi di privatezza che avevano fatto sorgere già allora. Oggi non c'è più bisogno di creare la "data centralen" con tutti i dati centralizzati, perché le banche dati stanno presso gli enti che ne sono proprietari, e l'accesso avviene in rete, in modo interoperabile tra un'amministrazione e l'altra: questo è il concetto della pubblica amministrazione estesa.

Per concludere, vorrei citare alcuni casi di realtà in cui mi trovo personalmente coinvolto e che stanno affrontando questo tipo di problemi.

Un primo esempio è quello dell'Istituto Nazionale per la Previdenza Sociale, che tramite i propri personal computer, ma anche tramite gli sportelli non presidiati che gradualmente vengono sviluppati, dà la possibilità di accedere sia alle banche dati previdenziali proprie, sia anche alle banche dati della pubblica amministrazione estesa. In particolare, tramite la rete INPS sono consultabili archivi come quello del fisco, degli infortuni, delle anagrafi comunali, delle utenze industriali. L'obiettivo è quello di ottenere degli incroci informativi, e questo ha dato e sta dando degli enormi risultati. Per esempio, per non pagare le pensioni alle persone decedute, mediante l'integrazione con le anagrafi comunali, oppure per fare in modo che chi ha trattamenti pensionistici presso diversi Enti abbia una ritenuta fiscale alla fonte che tenga conto di tutti questi diversi trattamenti.

Un altro caso è quello della Regione Lombardia, con il progetto "Lombardia integrata", che è qualcosa di simile alla rete unitaria della pubblica amministrazione a livello regionale. L'obiettivo è di integrare le anagrafi dei comuni e degli altri enti fra di loro, a livello regionale, in modo ad esempio che da un lato i dati stiano dove devono stare, ma possano essere interoperabili; dall'altro lato, la Regione, ad esempio, può essere preparata a gestire la fiscalità (come presto sarà chiamata a fare) e anche a fornire una porta di accesso verso l'amministrazione centrale. Per enti come l'INPS è veramente problematico gestire gli incroci con le anagrafi di quasi 10.000 comuni, è un problema che nessun ente centrale può risolvere da solo. Lo può risolvere tramite i corpi intermedi dell'amministrazione pubblica, tra-

mite ad esempio le Regioni che attuano questi progetti in rete.

Un altro esempio di progetto interoperabile che sta diventando operativo è quello, sempre in Lombardia, della sanità in rete con la carta intelligente. L'obiettivo è quello di dotare i cittadini di una carta intelligente multigestore, ma soprattutto di mettere in rete medici, farmacisti, ambulatori, ospedali, e la Regione stessa, in modo da avere, da un lato, una facilitazione nell'accesso ai servizi sanitari e dall'altro lato, anche un controllo della spesa sanitaria da parte degli organi regionali ad essa preposti.

Questo tipo di argomento, la sanità, pone dei problemi di privatezza molto più importanti degli altri settori, proprio perché stiamo gestendo dei dati sensibili, con una grossa differenza rispetto al caso delle transazioni bancarie o del commercio elettronico poiché in quel caso il fornitore del servizio, (la banca o il venditore), non ha il problema di non dover conoscere i dati relativi a che cosa ha ordinato quel cittadino, perché anzi il servizio consiste proprio nel fatto che il cittadino compra qualcosa dall'azienda o fa un'operazione finanziaria con la banca, e quindi non c'è una protezione di ciò che sta facendo quel cittadino. Nel campo sanitario la cosa è diversa.

Nel sistema articolato a livello regionale, lo scambio tra il paziente e il medico non deve essere conosciuto nella sua interezza da tutti gli attori coinvolti. Quindi c'è un problema di protezione molto più accentuato. Proprio per questo motivo, alla base di questo sistema c'è una sofisticazione molto elevata per i problemi di sicurezza. In quel caso, la carta intelligente diventa lo strumento da un lato per identificare la persona, ma dall'altro lato per svolgere tutte le funzioni di firma elettronica e di crittografia che sono necessarie per questo tipo di soluzione.

Infine, per concludere, citerò un ultimo progetto cooperativo: l'integrazione di servizi di tre enti, la Regione Lombardia, il Comune di Milano e la Camera di commercio di Milano. Si tratta di fare servizi integrati al cittadino e all'impresa da sportelli collocati presso queste amministrazioni, ma anche da sportelli automatici, collocati altrove, ad esempio presso le banche.

Si mettono prima in rete i servizi che già esistono, e poi si sviluppano nuovi servizi. Ad esempio, il Comune di Milano sta cominciando a sviluppare la carta di identità elettronica (la carta del cittadino), che dovrebbe evolvere verso un'unica soluzione con la carta sanitaria.

E qui si pone un ulteriore problema: quello di fare in modo che tutte queste iniziative di carte pubbliche che stanno sorgendo in vari contesti, in qualche modo alla fine convergano. Nel senso che non vogliamo avere una serie di carte differenti nel portafoglio, ma vorremmo avere possibilmente in prospettiva un'unica carta che serva come carta di identità elettronica, come patente, ma anche come carta sanitaria e perché no (dal momento che a tutto questo sono associati dei pagamenti), che serva anche come carta bancaria.

Abbiamo quindi la prospettiva di dover orientare con degli standards funzionali tutte queste diverse iniziative verso una convergenza, per evitare un'ulteriore proliferazione che ci porterebbe non alla interoperabilità, ma ad avere mondi separati; questi strumenti, da un lato le reti, dall'altro le carte intelligenti, servono non solo per interoperare, ma per garantire che l'identificazione, l'autenticazione dei messaggi, la sicurezza ottenuta tramite la critto-

grafia. Una grossa sensibilizzazione va fatta, proprio per evitare che nel desiderio di dare servizi migliori e più integrati nascano dei tipi di applicazioni dove non ci si preoccupa di mettere le necessarie sicurezze nel sistema fin dall'inizio.

La sicurezza, infatti, è un qualche cosa che va introdotta fin dal momento della progettazione e che non può essere facilmente inserita poi, successivamente, una volta che il sistema è realizzato.

Un ultimo commento: spesso le amministrazioni pubbliche dovranno cooperare con i privati per la distribuzione delle banche dati pubbliche; spesso dovranno esistere degli *information provider* che mettono assieme varie banche dati e attuano un servizio capillare che l'ente pubblico non sempre è in grado di svolgere, per dare un valore aggiunto all'informazione pubblica che esiste e che può essere distribuita.

Occorre preoccuparsi che mentre avviene questo, mentre gli *information provider* si sviluppano, vengano anche garantite le protezioni riguardo alla sicurezza e alla autorizzazione dell'accesso all'informazione, oltre che a normare la percentuale di costo che deve essere riconosciuta all'amministrazione pubblica per la gestione di queste informazioni, anche se esse vengono distribuite dai privati.

Questo discorso della distribuzione delle banche dati pubbliche tramite i privati, nel nostro Paese non ha trovato le modalità attuative necessarie. Alcuni Paesi come gli Stati Uniti con un atto di pubblicità dell'informazione, e altri Paesi come la Francia alcuni anni orsono, hanno normato questa distribuzione. Nel nostro Paese, nonostante ci siano state anche delle iniziative e delle proposte normative fatte negli anni scorsi a questo proposito, ancora non si è arrivati a una determinazione di come procedere; una soluzione è importante, perché man mano che le reti si sviluppano, sempre di più il ruolo dei fornitori di accesso privati diventa essenziale come complemento alla distribuzione diretta dei dati da parte dell'amministrazione pubblica.

Prof. Rodotà

Io ringrazio molto il prof. Bracchi per la precisione della sua esposizione, che pone moltissime questioni e non provo neppure a fare le domande che il suo intervento sollecita. Io mi limiterei a ricordare che proprio nell'ambito della delega prevista dalla legge 676, che ha accompagnato la disciplina generale, il punto riguardante questo tipo di carte è esplicitamente menzionato. Quindi è opportuno anzi che il legislatore delegato accentui l'attenzione per questo problema, proprio per evitare una proliferazione un po' incontrollata, perché si tratta non solo di prevedere misure di sicurezza, ma anche di prevedere quali sono i margini di decisione dei singoli cittadini rispetto a un passo così importante.

Vorrei poi richiamare l'attenzione su un punto particolarmente rilevante: il flusso delle

informazioni dal settore pubblico ai privati, perché il prof. Bracchi ha sottolineato la questione della scarsa attenzione in Italia per i fornitori privati di informazioni pubbliche. Questo è un punto sicuramente rilevante, che però va guardato a mio giudizio anche da un altro punto di vista. Può esserci il rischio che informazioni in mano pubblica di grande rilievo e acquisite tramite denaro pubblico vengano messe a disposizione in forme facilmente accessibili per i cittadini soltanto da parte di privati con costi non eccessivi rispetto alla prestazione, quindi l'attenzione deve essere anche rivolta al fatto che il ricorso al privato non deve significare per il pubblico negare il diritto di accesso dei cittadini.

Aggiungerei, come ultima considerazione, che nel momento in cui si discute molto di privatizzazioni, questo significa anche che una legge molto importante del nostro Paese, cioè la legge 241 con l'accesso ai documenti pubblici, vede ridotto l'ambito della sua applicazione, perché documenti prima qualificabili pubblici diventano privati.Si tratta dunque di un altro settore nel quale la privatizzazione deve essere accompagnata, laddove è necessario, da una riflessione sulla natura di questi dati per vedere se il passaggio al settore privato significa automaticamente opacità, oppure se il carattere comunque di interesse generale di questi dati debba essere salvaguardato.

Ma queste sono questioni complesse che l'interesse dell'intervento del prof. Bracchi mi spingeva a sottolineare.

Darei adesso la parola al prof. Alessandro Pace, ordinario di diritto costituzionale all'Università di Roma "La Sapienza" che molto modestamente dice di voler porre soltanto una domanda al prof. Poullet.

Prof. Alessandro Pace

Mi limito a prospettare un dubbio: un dubbio teorico. Non sono infatti un esperto di informatica. Anzi, non so far nemmeno funzionare un *computer*: tutt'al più il *data-base* tascabile. Oltre non vado.

Il dubbio ha la sua radice - e una sua spiegazione - in fatti autobiografici. Sono nato in una piccola città di provincia e quando, da adolescente, a sera, parlavo con mio padre, talvolta mi accorgevo - dalle domande che mi rivolgeva o dalle osservazioni che faceva - che egli sapeva dove e con chi ero stato durante la giornata. Ebbene, io non vedevo l'ora di da quell'ambiente provinciale, perché avvertivo che quel diffuso e impalpabile controllo sociale limitava la mia libertà. Sono perciò ben consapevole che il controllo sociale limita la libertà, e sin d'allora io volevo guadagnarmi la mia libertà.

Da cittadino adulto, e non solo da giurista, sono però a conoscenza di un dato incontestabile: nelle metropoli, dove il controllo sociale è senza dubbio minore (se non addirittura inesistente), la percentuale di reati è certamente superiore a quella delle città di provincia. Non già che anche in queste città non si compiano efferati delitti, ma la percentuale è

nettamente inferiore. Perché? Ma perché nelle città di provincia e nei minori aggregati urbani c'è quello "spiacevole" controllo sociale, diffuso e pervasivo. Il che, oltre tutto, dimostra che con i soli strumenti giuridici non si possono fronteggiare i comportamenti devianti.

Mi chiedo (e vi chiedo): ma, allora, un po' di controllo sociale è sempre un male?

Ho ascoltato con attenzione la relazione del prof. Poullet e ho appreso che la sigla PETS sta per tecnica di protezione della riservatezza del dato informatizzato. Orbene, se ho ben compreso, questi PETS potrebbero essere utilizzati per occultare non solo il contenuto dei messaggi, ma anche la provenienza degli stessi (e cioè l'identità del mittente). Ma, questa, è una scelta sensata e razionale o rischia invece di ritorcersi a danno della società in cui viviamo e dei singoli?

La segretezza del mittente non è tutelata, nel nostro ordinamento, allo stesso modo del contenuto del messaggio, anche quando la segretezza di questo messaggio è garantita - dall'art. 15 della nostra Costituzione - nei confronti dello Stato e dei terzi. Ancorché la Corte costituzionale abbia sostenuto il contrario, con riferimento alle sole comunicazioni telefoniche (sent. n. 81 del 1993), tuttora ritengo che la disciplina dei dati esteriori del messaggio (e cioè l'identità del mittente) vada distinta dalla tutela della segretezza del contenuto. A maggior ragione, la segretezza dei dati esteriori e del contenuto del messaggio non può dirsi tutelata con riferimento a quei messaggi (come quelli interpersonali a voce alta o come quelli contenuti nelle cartoline postali) che sono "manifestazioni" (e cioè pubbliche espressioni) di pensiero ancorché rivolte a un soggetto determinato: manifestazioni che perciò la nostra Costituzione protegge e disciplina nell'art. 21, e non nell'art. 15.

Ebbene: *Internet* - come è noto anche a un non esperto di informatica quale sono io - può servire da (e quindi essere) missiva chiusa, telefonata, cartolina postale o discorso pubblico, con conseguente applicabilità, a seconda del caso, dell'art. 15 e dell'art. 21.

Ecco allora a Voi, nuovamente, la mia precedente domanda, ma diversamente formulata: è giusto utilizzare la tecnica di protezione della riservatezza del dato, quando il dato, *ab origine*, è una "manifestazione"; come tale non coperta da segretezza? È giusto che per realizzare una effettiva libertà, si finisca per tutelare la riservatezza anche di dati o di comportamenti che di per sé non potrebbero essere qualificati come essenzialmente riservati? È giusto impedire il controllo sociale con riferimento a comportamenti non essenzialmente riservati e per i quali non si è scelta, dal mittente, una tecnica di trasmissione atta ad assicurare la segretezza del contenuto?

Questo è il problema; e questo è il dubbio che Vi sottopongo. Grazie.

On. Rodotà

Grazie ad Alessandro Pace, Poullet darà una risposta alla fine di questa sessione, ammesso che possa dare una risposta esauriente a una questione così grande.

La parola a Marco Gasparinetti, che ha una posizione strategica nell'Unione Europea, perché non è soltanto persona che ha molto lavorato e scritto in materia di tutela del consumatore in particolare, ma in questo momento, nella divisione del mercato interno, ha responsabilità relative alla libera circolazione delle informazioni e alla tutela dei dati personali. Lo ringrazio di essere qui e gli do la parola.

Dr. Marco Gasparinetti

Grazie prof. Rodotà per le parole gentili e grazie per l'invito a questo convegno, che cade a un anno circa di distanza dall'entrata in vigore della legge 675. In occasione di questo primo anniversario, vorrei innanzitutto rendere omaggio all'attività svolta dal Garante, il cui prestigio, anche sul piano internazionale, non ha tardato ad affermarsi, prova ne sia la recente nomina del prof. Rodotà alla Vice Presidenza del gruppo europeo dei Garanti per la protezione dei dati personali.

Il prof. Poullet poco fa ha già evidenziato alcuni degli aspetti su cui forse è opportuno che spenda qualche parola, anche se nei limiti di tempo che ci sono imposti.

In primo luogo, i problemi di interpretazione delle due direttive comunitarie già adottate in materia di protezione dei dati personali: la direttiva 95/46 del 24 ottobre 1995 e la direttiva 97/66, del 15 dicembre 1997, a proposito della quale dovrò spendere un' ulteriore parola di apprezzamento per il governo italiano in quanto, con ogni probabilità, l'Italia sarà uno dei primissimi Paesi a recepire questa seconda direttiva, grazie agli sforzi congiunti dell'Autorità Garante e del Ministero della Giustizia. Sappiamo che il decreto delegato è attualmente alla firma del Presidente della Repubblica.

Detto questo, credo sia importante articolare il ragionamento su due piani: innanzitutto quello dell'interpretazione, e qui sono d'accordo con il prof. Poullet. Le due direttive, alla stregua di altri testi comunitari, possono porre alcuni problemi di interpretazione.

Il secondo aspetto cui vorrei accennare, quanto meno in maniera succinta, è quello dell'applicazione di questi testi; applicazione più in generale di qualunque normativa,

nazionale o comunitaria in un ambito come quello di Internet, in cui il problema non è tanto quello di sapere se le regole esistenti si applicano, ma quali regole e soprattutto in che termini di effettività, visto che gli utenti di Internet si troveranno spesso confrontati a problematiche complesse di diritto internazionale privato, per non parlare dei costi e della durata di un'azione "transnazionale" in giudizio. Questo, sicuramente, è uno degli elementi che militano in favore dell'esistenza di un Garante per la protezione di dati personali.

Per ritornare all'interpretazione delle due direttive, la direttiva-quadro del 1995 è "tecnologicamente neutra" e si applica senza alcun dubbio ad Internet, ed alle altre reti telematiche, anche se è vero che alcuni problemi di interpretazione possono porsi e il prof. Poullet ne ha identificati alcuni.

Per quanto riguarda i *cookies*, in particolare, non posso resistere alla tentazione di dare una primissima risposta, anche se questa risposta la darò a titolo personale (come sapete, l'interpretazione autentica del diritto comunitario spetta alla Corte Europea di giustizia, ed in quanto funzionari della Commissione europea, noi possiamo solo esprimere un apprezzamento e un'opinione a titolo personale). A mio parere, l'articolo 4 lettera *c)* della direttiva 95/46 consente l'applicazione della normativa europea, e quindi della normativa nazionale che recepisce la direttiva, in relazione ai dati personali raccolti dai *cookies* a partire da uno stato terzo, e questo perché i *cookies* interagiscono col disco duro dell'utente. Il fatto è che il "cooky", per le modalità tecniche che sono state correttamente individuate dal prof. Poullet, consente di utilizzare un supporto che è a disposizione dell'utente e che si trova nel territorio di uno Stato membro dell'Unione europea, e questa situazione ricade nell'ambito di applicazione della direttiva 95/46.

La definizione di "dati personali", che determina l'ambito di applicazione della direttiva quadro, è estremamente ampia. Tale definizione è tale da ricomprendere qualunque dato che possa portare direttamente o indirettamente alla identificazione di una persona, in particolare mediante riferimento a un numero di identificazione.

Vero è che alcuni aspetti relativi ad Internet meritavano una normativa più dettagliata, e questo è uno dei motivi per cui, il 15 dicembre 1997, il Consiglio e il Parlamento Europeo hanno adottato una direttiva specifica sulla protezione dei dati personali nel settore delle telecomunicazioni, che integra e completa la direttiva "quadro" del 1995.

Questa seconda direttiva si applica unicamente ai servizi di telecomunicazione accessibili al pubblico. Una definizione importante in relazione a quanto esposto questa mattina, perché questo significa che la direttiva 97/66 si applicherà sicuramente ai servizi offerti su Internet (che, per definizione è una rete aperta) ma non si applicherà probabilmente ad altre reti telematiche, che vengono invece definite come sistemi "proprietari".

Alcuni esempi di sistemi proprietari credo siano ben noti: uno è quello che consente alle banche di gestire le transazioni finanziarie effettuate ad esempio con una carta Bancomat. Questo è un sistema chiuso, non accessibile al pubblico: non è che chiunque possa accedere ai dati contenuti negli archivi delle banche, o a quelli del sistema sanitario nazionale, soprattutto se si tratta di archivi elettronici.

Un altro esempio di sistema proprietario è quello delle prenotazioni computerizzate

che viene gestito dalle compagnie aeree. Al proposito vorrei citare un aneddoto recente a cui la stampa inglese ha dato ampio rilievo: nel Regno Unito si sono verificate, all'inizio di quest'anno, una serie di furti in abitazioni di persone che erano partite per un viaggio, e il numero di questi furti era tale che a un certo punto Scotland Yard ha cominciato a interrogarsi sulla possibilità che qualcuno avesse accesso alle prenotazioni effettuate dalle persone che erano partite in viaggio. Le indagini hanno permesso di accertare che, in effetti, persone non autorizzate avevano accesso al sistema di prenotazioni della British Airways, con la conseguenza che molte case avevano ricevuto delle "visite" indesiderate in assenza dei legittimi proprietari.

Un'altra forma di "controllo sociale" non auspicabile è quella che ha recentemente attirato l'attenzione dei media negli Stati Uniti, e qui parliamo di un altro sistema di banche dati: le farmacie ed altri operatori del servizio sanitario avevano preso l'abitudine di vendere i dati relativi al consumo di prodotti farmaceutici ad alcune aziende, che potevano essere interessate ad effettuare campagne di marketing diretto. Risultato: alcune migliaia di consumatori americani hanno ricevuto, all'inizio di quest'anno, una lettera che molto gentilmente ricordava come, nel 1978, il destinatario della missiva aveva sofferto della malattia xxx, che nel 1982 aveva fatto uso smodato del medicinale yyy e così via. Questo per vantare i meriti di un nuovo prodotto che l'azienda farmaceutica in questione intendeva mettere sul mercato e che avrebbe rappresentato la panacea per tutti i mali di cui sopra. Credo che questo tipo di schedatura sia abbastanza fastidioso dal punto di vista delle persone che hanno ricevuto la missiva: non a caso, a seguito di una campagna di stampa estremamente dura che ha denunciato il fenomeno, l'azienda in questione ha sospeso l'operazione.

L'esempio ci ricorda che un'altra categoria di sistemi "proprietari", il sistema sanitario nazionale, rappresenta una fonte potenziale di dati che sicuramente devono essere protetti. Questo non sulla base della direttiva 97/66, ma sulla base della direttiva quadro, la 95/46, che impone fra l'altro un obbligo di sicurezza a carico del responsabile del trattamento, obbligo di sicurezza che si traduce anche nella necessità di proteggere i dati conservati, in particolar modo per quanto concerne i dati sensibili.

Altri esempi sono stati fatti questa mattina: esempi che non sono coperti dalla direttiva 97/66, ma lo sono sicuramente dalla direttiva quadro. Il Prof. Rodotà ha già fatto riferimento alle "smart cards", o carte "intelligenti": talmente intelligenti che se qualcuno riuscisse ad avere una lista di tutte le transazioni o le comunicazioni effettuate con queste carte, la situazione potrebbe degenerare in uno scenario da "grande fratello" (*big brother*) di orwelliana memoria. Tutti noi abbiamo probabilmente due o tre di queste carte: la carta Bancomat è un esempio, ma anche nei telefonini è contenuta una carta, la carta SIM, che consente di sapere quali comunicazioni sono state effettuate e quali comunicazioni ricevute.

A mio parere, l'esempio forse più interessante è tuttavia quello delle *smart cards* che potranno essere utilizzate per fruire dei servizi offerti dalla televisione digitale. Si parla molto di dei vari settori dell'industria della comunicazione: telecomunicazioni, televisione e informatica e così via; questo per sottolineare che presto sarà possibile, con uno stesso apparecchio, con una stessa tecnologia, avere accesso a Internet e ai programmi televisivi,

perché la tecnologia è la stessa, la tecnologia digitale. Come dice Negroponte, si tratta sempre di *bytes*: la trasformazione di suoni, dati e immagini è un semplice impulso elettronico, di natura binaria, che rende irrilevante il metodo di trasmissione.

Ora, con questo tipo di *smart card* sarà possibile (per il fornitore del servizio) avere una lista dei programmi televisivi, o dei servizi Internet, che il singolo utente avrà deciso di fruire, il che potrà anche essere necessario ai fini della fatturazione: la *pay per view* è una delle possibilità che già viene utilizzata, ad esempio, nelle grandi catene alberghiere. Il prof. Rodotà ricordava a giusto titolo quanto sia necessario riflettere a questi aspetti, e come le carte intelligenti presentino una doppia faccia: nuovi servizi e comodità di utilizzo per il consumatore, ma anche maggiori possibilità di "controllare" gli utenti in ogni singolo gesto della vita quotidiana.

A questo proposito, sull'interpretazione della direttiva 95/46 non ci sono molti dubbi: il trattamento dei dati personali che sarà possibile in questi ambiti è sicuramente coperto dalla direttiva, e questo si traduce in modo particolare nei diritti soggettivi che vengono riconosciuti dalle disposizioni già recepite nell'ordinamento italiano: il diritto di accesso, il diritto di rettifica e il diritto di opposizione in particolare.

Tuttavia, introdurre diritti e obblighi non basta se poi questi restano sulla carta: la persona può essere sicuramente turbata dalla violazione della propria riservatezza, subirla come un affronto, ma quanti di noi o quante persone ordinarie si rivolgerebbero poi ad un avvocato per far causa ad un "webmaster" che si trova negli Stati Uniti, in Giappone, in Afghanistan o altrove? I costi di un'azione e i tempi della giustizia ordinaria sono tali che probabilmente la stragrande maggioranza delle violazioni al diritto alla riservatezza resteranno impunite. E su questo vorrei concludere per riaffermare la validità del modello europeo consacrato dalla direttiva, ma che in parte preesisteva in vari Paesi membri dell'Unione Europea; quello cioè di un'autorità garante e indipendente: garante dell'effettività della norma, in una materia che attiene ai diritti fondamentali della persona, e indipendente rispetto alle pressioni dei tanti piccoli o grandi fratelli per i quali i dati personali (quelli altrui) sono soltanto una merce fra le tante.

On. Rodotà

Credo che tutti abbiano avuto modo di apprezzare la precisione e la chiarezza del dott. Gasparinetti che noi che lavoriamo ogni tanto con lui conoscevamo già.

Do la parola con molto piacere e un po' di paternalismo alla dottoressa Valentina Gripo. Paternalismo perché la dott.ssa Gripo si è laureata con me e con me continua a lavorare.

Dott.ssa Valentina Gripo

Provo un po' di imbarazzo a parlare con le persone che hanno scritto i testi che ho studiato fino adesso e vorrei riportare soprattutto le riflessioni che mi derivano dal fatto di essere un utente di Internet prima ancora che una persona che si appassiona a questi temi.

Nella sua relazione, il prof. Rodotà ha annunciato come esistano e siano in corso di emanazione una serie di normative a disciplina di Internet, però ancora adesso sentivo dire che queste leggi avranno l'effetto di paralizzare Internet, che Internet non sia da regolamentare o, ancora più forte, non sia fisicamente regolamentabile e che comunque una regolamentazione sfuggirà di mano perché non si potrà applicare.

Questa è una sensazione che viene per chi si trova a trafficare con i dati, con la quantità di dati che si possono reperire su Internet.

Questo problema è come un mezzo di comunicazione unico, in cui circolano dati omogenei, ma si risolve, se si tiene conto del fatto che Internet come è stato descritto molto bene dalla sentenza della Corte Suprema già citata sulla *communication decency act*, è un mass media a possibilità multipla.

Quando si chiede che regola si debba applicare ad Internet, bisogna tenere conto del fatto che Internet è al tempo stesso un telefono, è una lettera, può essere un televisore, è un giornale, è una piazza, come è stato sottolineato nella sentenza, ed è anche un mercato elettronico, un *electronic shopping mall*, come lo ha chiamato Al Gore nella sua relazione del '95.

Tutti questi modi di essere di Internet sono caratterizzati dalla circolazione di dati personali diversi, che sono o a mio avviso devono essere soggetti a una disciplina diversa e solo in questo modo si può pensare a una regolamentazione di Internet; se lo si continua a guardare come un blocco unico, effettivamente sfugge un po' di mano come si debba regolamentare.

Così, ad esempio, se si guardano i contenuti dell'MI sono già protetti dal codice penale oltre che dalla Costituzione, come ha evidenziato il prof. Pace nel suo intervento, si tratta

di strumenti diversi, che richiedono una forza diversa di protezione a seconda di quale è il diritto che viene esercitato in diversi utilizzi di Internet.

Allo stesso modo i dati sul traffico, i cosiddetti *transactional data*, sono disciplinati dalla direttiva prima citata, dalla 97/66, e penso che verranno presto recepiti dal decreto in emanazione, per cui verranno presto regolamentati anch'essi dalla normativa italiana, contemporaneamente a quella europea.

Rimangono aperti due problemi ed è su questi che in futuro bisognerà soffermarsi e sono emersi chiaramente dalla relazione del prof. Poullet.

Il primo si riferisce alla disciplina normativa del monitoraggio degli spostamenti degli utenti online. Come abbiamo visto, dal punto di vista tecnico questo è possibile, viene fatto costantemente, ed è possibile anche molto di più di quello che viene fatto costantemente. I cookies attualmente sono utilizzati, ma in futuro i *cookie*s, i programmi spider, tutto il caso che è emerso intorno al Microsoft Wave, il Java, ci sono una infinità di strumenti tecnici, che danno la possibilità di monitorare quello che uno fa quando si muove come utente all'interno delle reti.

Dal punto di vista teorico si parla di passaggio da un sistema push a un sistema pull, da un sistema nel quale l'utente accende il computer, si collega su Internet e si va a cercare le informazioni che gli interessano, a un sistema nel quale è Internet che spinge sul suo computer i dati che secondo lui dovrebbero interessare l'utente. Io accendo il mio computer, il mio computer mi dice: è uscito un nuovo articolo su Internet, tu hai un bambino piccolo, c'è un nuovo sito che parla dei problemi delle giovani madri e in più ti occupi di ippica. Questa cosa ha dei vantaggi reali perché molti di noi, come utenti, si sono accorti che ci si perde su Internet a cercare le informazioni a cui si è interessati, per cui è chiaro che un sistema di questo tipo non è che sia da condannare a priori in nome della privacy. Vero è che, come enunciava il prof. Poullet, è necessaria una consapevolezza da parte dell'utente di quello che fa quando si muove per Internet: nel momento in cui l'utente è posto in posizione paritaria rispetto al fornitore di questo servizio, è chiaro che questo servizio ben venga perché aiuta l'utente, però l'utente deve sapere che sta dando quella informazione e che in base a quella informazione riceverà in cambio altre informazioni.

A questo proposito vorrei fare un breve inciso: la regolamentazione e gli strumenti di self regulation, le PETS e così via, non sono cose alternative, almeno la mia impressione è questa; facendo un esempio del prof. Simitis, il fatto che le automobili abbiano i freni e abbiano un limite fisico di velocità non vuol dire che non debbano esistere leggi che impongono dei limiti di velocità, sono due cose diverse, che viaggiano parallelamente e che è auspicabile si aiutino l'un l'altra.

Il secondo punto del quale si è sempre parlato molto e del quale non si può non parlare quando si parla di Internet, è relativo alla necessità di una regolamentazione sovranazionale, di un quadro di principi generali non solo europei, ma globali che prescindano dalle regolamentazioni che pure sono molto avanzate dei singoli Paesi. È stato detto, e su questo non sono molto d'accordo, che Internet pone dei problemi analoghi al falso o ad altri sistemi che consentono di trasmettere grandi quantità di dati.

In realtà, come è stato illustrato dal prof. Poullet, questo non è del tutto vero, perché tramite i *cookies* potrebbe essere che io, utente, do delle informazioni a un computer che, fisicamente, sta da tutta un'altra parte e che questi dati sono elaborati, trattati, schedati e riutilizzati per farmi un'offerta commerciale o simile, e tutto questo avvenga tutto al di fuori della mia nazione, per cui servirebbe una specie di accordo sovranazionale di principio, non solo per evitare che ci siano quelli che sono stati chiamati paradisi informatici, una nuova generazione di paradisi informatici, ma anche che ci siano dei Paesi, al di fuori dell'Unione Europea, che facciano un ragionamento già fatto da Robert Bosch in un eloquente articolo, *Keep privacy law out of cyberspace*, a commento della direttiva del '95, in cui lui invitava gli Stati Uniti a mantenere un livello di tutela inferiore a quello europeo, affinché la disciplina della privacy sviluppasse, avvantaggiasse le aziende americane rispetto a quelle europee.

Questo, anche in virtù della relazione che è stata fatta prima dal prof. Bracchi rispetto allo sviluppo delle aziende su Internet; è chiaro che la privacy non può diventare uno strumento per indebolire la posizione delle aziende europee su Internet rispetto ai concorrenti americani.

Prof. Rodotà

Molte grazie a Valentina Gripo per queste sue osservazioni molto pertinenti. Prima di dare la parola al Prof. Poullet per una breve replica, Giovanni Buttarelli voleva rivolgergli due domande.

Cons. Giovanni Butarelli

Segretario Generale, Garante per la protezione dei dati personali

Vorrei rivelare un dato sensibile e cioè che l'apprezzato prof. Poullet è impegnato in una interessante attività di ricerca su Internet e vorrei quindi esercitare il nostro diritto di accesso ai dati di cui lui è in possesso.

Le domande riguardano l'anonimato. Il gruppo europeo che racchiude le autorità garanti sulla privacy, citato da Gasparinetti, ha approvato un documento importante sull'anonimato, distribuito a tutti voi, nel quale si danno delle indicazioni molto ferree per garantire anche in Internet il diritto all'anonimato, soprattutto per l'uso delle e-mail, per il *browsing* passivo e per l'acquisto di molti beni e servizi.

In questo documento, però, si dice che l'anonimato andrebbe in qualche modo bilanciato con altre esigenze.

Noi, in Italia, con questo decreto legislativo che è in corso di pubblicazione, abbiamo dato largo spazio all'anonimato e questo permetterà ad esempio ad un lavoratore di avere accesso anonimo a Internet dal posto di lavoro in una pausa di lavoro.

Dai dati di cui il prof. Poullet è in possesso nella sua ricerca, come bilancerebbe questo anonimato con queste altre esigenze pubbliche? Soltanto nei casi di reato? In altri casi di controversia giudiziaria? Quali sono le sue esperienze su questo punto?

Il secondo aspetto riguarda come identificare le persone che vogliono rimanere anonime, affinché, in caso di necessità, quando occorre bilanciare queste esigenze, la persona possa essere identificata, perché molti *provider* adottano la tecnica di acquisire una fotocopia di un documento di identità, che però è facilmente falsificabile, altri provider si rifiutano di identificare gli utenti; altri provider ancora sostengono che ormai un abbonamento via Internet si può concludere per via elettronica e che quindi l'identificazione è molto difficile.

La seconda domanda riguarda le tecniche concrete per identificare i soggetti che vogliono e debbono rimanere anonimi, ma che in caso di necessità, in casi molto selezionati, potrebbe essere utile identificare. E lo ringraziamo per le risposte.

Prof. Yves Poullet

Une partie de la question de Monsieur Buttarelli rejoint la question de l'intervenant précédent et je m'empresse de leur répondre à tous deux.

Habitant moi-même un village, je suis fort sensible à leur comparaison entre le village global et virtuel que représente Internet et le village réel. Sans doute, là comme ici, chacun s'exprime librement, sous le contrôle d'autrui et ce n'est pas plus mal car le contrôle d'autrui est sans doute la meilleure manière de moraliser le comportement de chacun.

La comparaison est trompeuse et dangereuse. Ce qui caractérise mon village, le réel, c'est qu'à côté de chez moi, je sais qu'habitent deux vieux célibataires, lesquels sont friands de voitures étrangères et que si unjour un étranger vient chez moi, je devine que deux jours après tout le monde le saura. Je connais le regard d'autrui et si cela me déplaît, je puis m'en prémunir, le contrer. C'est cela la vie en Société. Savoir que l'on vous regarde, mais pouvoir contrôler l'image que l'on donne de soi.

Sur Internet, mon "village virtuel", je ne sais pas qui m'observe, je n'ai aucun contrôle de l'utilisation qui sera faite de l'information qu'y promenant j'y crée. Le contrôle de mon image se perd et sans doute est-ce pour cela que des législations me rendant la possibilité d'une telle maitrise sont si importantes.

Un second point est évoqué : ne faut-il pas établir des réglementations à géométrie ou

plutôt rigueur variables selon la sensibilité des données. La visite d'un site pornographique crée certes une donnée plus sensible que ma visite de la bourse sur le site Web du Washington Post. Cependant, et le contexte d'Internet le permet (cf. le cas de Double Click évoqué dans ma présentation), une donnée même banale connectée avec une multitude d'autres données venant d'horizons extrêmement différents permet de définir de manière extrêmement précise le profil d'un individu voire de l'utilisateur d'un browser X et cela est peut-être bien plus dangereux que la simple information relative à la visite d'un site pronographique.

A l'inverse, et j'en viens à une troisième question, les données publiques méritent également une protection et c'est à raison, me semble-t-il, que la directive ne prévoit pas d'exceptions en ce qui les concerne. Stefano Rodota en a parlé tout à l'heure. Dans le contexte d'Internet, cette question des données publiques prend encore une autre dimension. Les données que je publie sur moi-même, que je mets sur mon propre site ou celui de mon employeur, ne peuvent être utilisées par autrui sans limites. Actuellement, et le Groupe International de Protection des Données sur les Télécommunications et la vie privée (le Groupe de Berlin) va travailler sur ce point - des robots de recherche tels Infoseek ou Altavista, opèrent un de l'infinité des diverses pages Web présentes et vous permettent de tirer un profil précis de la personnalité de quelqu'un. Il a dit ceci, il a été là, il a publié cela. Par ailleurs, on peur imaginer que votre page Web que vous destinez à vos collègues universitaires puisse être utilisé pour des raisons de marketing y compris politiques ou autres.

Enfin, faut-il publier sur Internet, des données telles que les décisions judiciaires. Un arrêté royal a été pris récemment en Belgique pour décider de la publication de tous les arrêts de la plus haute juridiction administrative. Je crois que la publication des noms des parties en particulier présente un danger au vu des possibilités de croisement des données et de traitement que permet l'informatique. Ainsi, si je veux la liste de tous les ayant recouru contre l'Etat pour refus de promotion, je puis facilement l'obtenir.

Une quatrième question portait sur l'obligation de chacun d'assurer sa propre sécurité pour assurer la confidentialité de ses propres messages. La comparaison entre l'envoi d'une carte postale de préférence à une lettre fermée était particulièrement évocatrice à cet égard.

Une réponse en deux temps, si vous le permettez. L'intervenant a raison d'insister sur la responsabilité des utilisateurs. L'interactivité d'Internet accroît cette responsabilité dans la mesure où c'est à lui à chaque étape de consentir. Sans doute, et ici cela ne dépend plus de lui mais des obligations que la société fera peser sur l'interlocuteur de l'utilisateur - faut-il qu'il soit pleinement informé des risques que lui, utilisateur, prend en consultant et des solutions qui existent pour les éviter.

Sans doute et c'est une seconde responsabilité de la société, faudra-t-il en outre que les mesures de sécurité, la cryptographie, l'anonymisation, bref, les PETS soient disponibles pour l'utilisateur à un prix raisonnable. C'est l'idée de étendu qui permet d'obliger les autorités de certification à offrir des procédés de signature électronique à ces coûts abordables pour certaines catégories sociales.

Enfin, ne faut-il pas exiger que les systèmes techniques soient par défaut configurés de

manière à offrir cette sécurité (ex. que le filtrage des cookies soit automatique) et que le recours à ces systèmes ne pénalisent pas trop l'utilisateur (ainsi actuellement, le filtrage des cookies à l'entrée permis par les dernières versions des browsers reste une tâche lourde).

Je voudrais en venir enifn au problème de la sécurité publique. C'est vrai que grâce à des techniques d'encryptage, grâce à des techniques d'anonymisation, on peut dire que les "brigands" se voient faciliter leur travail. Ce que je crains c'est que, précisément à l'encontre de cette crainte, les autorités de police, pour des raisons très légitimes, à savoir la sécurité publique, ne développent des mesures qui soient disproportionnées par rapport au risque qu'il faut éviter.

Récemment, je rencontrais les représentants de l'autorité de protection des données hollandais. Ils m'expliquaient que pour avoir une carte mobilophone prépayée, l'autorité de police exige en Hollande que les personnes qui offrent ces cartes prépayées exigent la carte d'identité et gardent pendant trois mois la possibilité de réidentifier celui qui a utilisé cette carte prépayée, soi-disant anonyme.

Même problème avec les Internet access provider, qui se voient de plus en plus sous la pression des polices nationales et des gendarmeries nationales. On leur demande de garder une trace des utilisations faites par les internautes. D'un point de vue strictement de protection de la vie privée, les Internet access providers, dans la mesure où ils font payer un prix forfaitaire n'ont pas besoin de garder ces traces qu'on leur réclame de garder pour des raisons de sécurité publique. Ces traitements voulus pour des raisons de sécurité publique me semblent évidemment disproportionnés par rapport à l'équilibre qui existait dans le temps. A un moment donné, dans le cadre d'une instruction judiciaire, le magistrat ordonne une écoute de telle ou de telle ligne. La possibilité maintenant de pouvoir exiger des stockages de données a priori, indépendamment d'un problème bien particulier de mise en cause de la sécurité publique, m 'apparaît beaucoup aller à l'encontre de la jurisprudence du Conseil de l'Europe (art. 8) qui prohibe toute mesure a priori, globale et sans lien direct entre une infraction commise et les éléments permettant d'en retrouver l'auteur.

Dernière réflexion - et j'en resterai là - je l'ai affirmé, nombre de traitements opérés dans le cadre d'Internet, pourraient être visés par la directive Telecom et Privacy. Or, on le sait, cettte directive n'opère pas de distinction entre la protection des personnes morales et des personnes physiques, alors que la directive générale le fait. Bref, par ce biais, même si nombre de pays - l'Italie est une exception notoire - se refuse à protéger les personnes morales, ils pourraient bien être forcés de leur accorder cette protection, chaque fois que la directive Telecom et Vie Privée trouve à s'appliquer et à mon avis, ce sera souvent le cas. Bref, cela relance le débat sur l'opportunité de maintenir une distinction entre personne morale et personne physique, ce qui est heureux.

Prof. Yves Poullet

La domanda posta dal Dr. Buttarelli si ricollega in parte a quella formulata nel precedente intervento, e cercherò di rispondere ad entrambe.

Sono ben consapevole, abitando in un paesino, del confronto qui istituito fra villaggio globale e virtuale, rappresentato da Internet, e villaggio reale. Indubbiamente, in un caso come nell'altro, ognuno si esprime liberamente sotto il controllo altrui e ciò non è troppo negativo, poiché il controllo altrui rappresenta senza dubbio il modo migliore per moralizzare il comportamento dei singoli.

È un confronto fittizio e pericoloso. Quello che caratterizza il mio villaggio, quello reale, è il fatto di sapere che accanto a casa mia abitano due scapoli che hanno la passione delle automobili straniere, e se uno straniero viene a casa mia posso prevedere che entro due giorni lo saprà tutto il mondo. So chi mi guarda e se non mi va, posso difendermi, oppormi. Questo è il vivere sociale. Sapere che c'è chi ci guarda, ma poter controllare l'immagine di sé.

Su Internet, il "villaggio virtuale", non so chi mi osserva, non ho alcun modo di controllare l'utilizzo che verrà compiuto delle informazioni alle quali dò origine passeggiando per le sue strade. Si perde il controllo della propria immagine, e indubbiamente è per questo che assumono tanta importanza le norme che restituiscono la possibilità di tale controllo.

Secondo punto richiamato: se sia necessario stabilire norme a geometria, o meglio, a rigore variabile in rapporto alla sensibilità dei dati. Il fatto di visitare un sito pornografico costituisce indubbiamente un dato più sensibile del fatto di consultare i dati relativi alla borsa sul sito Web del Washington Post. Comunque, e il contesto di Internet lo consente (v. il caso di Double Click citato nella mia presentazione), un dato anche banale collegato ad una molteplicità di altri dati provenienti da ambiti del tutto diversi permette di definire con grande precisione il profilo di un soggetto ovvero dell'utente di un browser X, e ciò può ben essere più pericoloso della semplice informazione relativa alla frequentazione di un sito pornografico.

Peraltro, e vengo ad un terzo punto sollevato durante la discussione, i dati pubblici sono egualmente meritevoli di protezione, e mi sembra corretto che la direttiva non preveda eccezioni al riguardo. Stefano Rodotà ne ha appena parlato. Nell'ambito di Internet, questo tema dei dati pubblici acquista un'ulteriore dimensione. I dati che rendo pubblici sulla mia persona, che metto sul mio sito o su quello del mio datore di lavoro, non possono essere utilizzati da terzi senza alcun limite. Attualmente, e il Gruppo internazionale sulla protezione dei dati, le telecomunicazioni e la privacy (il Gruppo di Berlino) si occuperà del tema, motori di ricerca come Infoseek o Altavista operano uno delle infinite pagine Web presenti e consentono di ricavare con precisione un profilo della personalità di un soggetto determinato. Ha detto così, è stato colà, ha pubblicato quello... Peraltro, si può immaginare che la pagina Web da voi destinata ai vostri colleghi universitari possa essere utilizzata per fini di marketing, anche politici o di altra natura.

Infine, se si debbano pubblicare su Internet dati come le decisioni giudiziarie. Di recente è stato emanato in Belgio un decreto reale per regolamentare la pubblicazione di tutte le decisioni della massima autorità giudiziaria amministrativa. Credo che la pubblicazione dei nominativi delle parti in causa presenti in particolare un rischio alla luce delle possibilità offerte dalla tecnologia informatica di incrociare i dati e di eseguire trattamenti ulteriori. Così, se desidero l'elenco di tutti i "funzionari" che hanno presentato ricorso contro lo Stato per mancata promozione, posso ottenerlo con facilità.

Un quarto punto verte sull'obbligo per ciascuno di noi di garantirsi sicurezza per garantire la segretezza dei propri messaggi. Il confronto fra l'invio di una cartolina anziché di una lettera in busta chiusa era particolarmente evocativo a questo proposito.

Se permettete, vorrei articolare la risposta in due tempi. Il collega che è intervenuto ha ragione ad insistere sulla responsabilità degli utenti. L'interattività di Internet aumenta tale responsabilità nella misura in cui spetta all'utente acconsentire ad ogni tappa del proprio cammino. Indubbiamente, e ciò non dipende più dall'utente stesso, ma dagli obblighi che la società farà ricadere sull'interlocutore dell'utente, bisogna che sia informato appieno dei rischi che, in quanto utente, si assume effettuando la consultazione, e delle soluzioni possibili per evitarli.

Senza dubbio, e questo rappresenta una seconda responsabilità per la società, bisognerà inoltre che le misure di sicurezza, la crittografia, l'anonimizzazione, in breve le PETs, siano disponibili per gli utenti a costi ragionevoli. È il concetto di esteso che consente di obbligare le autorità di certificazione a offrire procedure di firma elettronica a costi abbordabili per determinate categorie sociali.

Infine, se sia necessario esigere che i sistemi tecnologici siano per default configurati in modo da offrire tale sicurezza (ad es., che il filtraggio dei cookies avvenga in modo automatico) e che il ricorso a tali sistemi non penalizzi troppo l'utente (ad esempio, attualmente il filtraggio dei cookies all'ingresso consentito dalle ultime versioni dei browser risulta una funzione pesante).

Vorrei affrontare infine il problema della sicurezza pubblica. È vero che, grazie a tecniche di cifratura, grazie a tecniche di anonimizzazione, si può affermare che i "malviventi" si sono visti facilitare le proprie attività. Quello che temo è che, proprio dinanzi a tale rischio, le autorità di polizia, per ragioni perfettamente legittime, ossia per ragioni di pubblica sicurezza, introducano misure sproporzionate rispetto al rischio che si intende evitare.

Di recente ho avuto un incontro con i rappresentanti dell'autorità olandese per la protezione dei dati. Mi spiegavano che per ottenere una carta prepagata per telefoni cellulari la polizia olandese chiede che i rivenditori esigano dall'acquirente l'esibizione della carta di identità, e conservino per tre mesi la possibilità di rintracciare il soggetto che ha utilizzato la carta in questione - cosiddetta "anonima".

Lo stesso ordine di problemi si presenta oggi per i fornitori di accesso a Internet, che si trovano sempre più esposti alla pressione degli organi di polizia nazionali e delle autorità di pubblica sicurezza le quali chiedono di conservare traccia degli utilizzi compiuti dagli internauti. Da un punto di vista strettamente connesso alla protezione della privacy, il fornitore

di accesso a Internet, nella misura in cui addebita un costo forfettario, non ha alcun bisogno di conservare tale traccia. È una richiesta motivata con esigenze di pubblica sicurezza.

Questi trattamenti richiesti per motivi di pubblica sicurezza mi sembrano chiaramente sproporzionati rispetto all'equilibrio esistente nel tempo. A un dato momento, nell'ambito di un'inchiesta giudiziaria, il magistrato dispone l'intercettazione di questa o quella linea; ebbene, la possibilità di chiedere la memorizzazione di dati a priori, indipendentemente dall'esistenza di uno specifico problema che riguardi la sicurezza pubblica, mi sembra sostanzialmente in conflitto con la giurisprudenza del Consiglio d'Europa (art. 8) che vieta ogni provvedimento a priori, di natura generale e in assenza di un legame diretto fra un certo reato e gli elementi che consentono di identificarne il responsabile.

Ultima considerazione - e qui mi fermerei - come ho già detto, un buon numero di trattamenti effettuati su Internet potrebbero essere coperti dalla direttiva su TLC e privacy.

Ebbene, è noto che questa direttiva non fa alcuna distinzione in termini di protezione fra persone giuridiche e persone fisiche, mentre tale distinzione è contenuta nella direttiva quadro. In breve, su questo fondamento, anche se alcuni paesi - l'Italia fa eccezione, come sappiamo - si rifiutano di tutelare le persone giuridiche, potrebbe indubbiamente sussistere l'obbligo di accordare alle persone giuridiche la tutela suddetta ogniqualvolta trovi applicazione la direttiva su TLC e privacy, e a mio giudizio ciò si verificherà di frequente. Dunque, tutto ciò rilancia la discussione sull'opportunità di mantenere una distinzione fra persone giuridiche e persone fisiche, il che è auspicabile.

II SESSIONE

Prof. Giuseppe Santaniello

Diamo inizio ai lavori della seconda sessione. Comunico che per un impedimento sopraggiunto, il Ministro Maccanico non può partecipare al Convegno e per mio tramite rivolge a tutti gli intervenuti un cordiale saluto.

Rivolgo un mio deferente e fervido saluto agli illustri relatori di questa sessione, l'on. Vincenzo Vita, sottosegretario al Ministero delle Comunicazioni, la prof.ssa Samuelson della Berkeley University, il prof. Oliva della Denison University.

Vorrei prospettare alcune brevi considerazioni introduttive al tema, che non intendono entrare nel merito dei problemi perché è compito fondamentale e preminente dei prestigiosi relatori, ma soltanto tracciare una linea di cornice nel quadro tematico di cui oggi ci occupiamo: la proprietà intellettuale in Internet.

Il nucleo tematico della proprietà intellettuale che in tutti i Paesi si caratterizza per la rilevanza culturale, economico-sociale, acquista un interesse ancora maggiore quando si riferisce a una rete di comunicazione quale Internet, la quale costituisce un sistema dotato di una capacità illimitata di diffondere idee, messaggi, simboli, immagini e rappresenta una vetrina mondiale di prodotti e di servizi immateriali.

Certamente Internet ha caratteristiche inedite e peculiari, che mettono in crisi la strumentazione giuridica corrente, poiché la dimensione intermediatica, acentrica e delocalizzata e la sua polifunzionalità, il suo polimorfismo ci obbligano a confrontare i fondamenti giuridici dei vari ordinamenti in una visuale innovativa. E ci impegnano soprattutto a ragionare in termini transnazionali.

Se non riuscissimo a rinvenire soluzioni valide per un quadro di regole universalmente accettate, Internet rischierebbe di diventare (come da altri è stato già detto) un Giano Bifronte, cioè una deità dal doppio viso, per cui il mezzo tecnologico potrebbe essere suscettibile di utilizzazioni di segno positivo o negativo al tempo stesso.

Proprio questa mattina il prof. Poullet ha tracciato un'analisi approfondita del duplice aspetto di Internet: l'aspetto positivo, l'aspetto chiaro, il volto palese e anche alcuni tratti del volto nascosto.

Ma noi abbiamo fiducia che tale rischio sarà scongiurato. Attraverso recenti linee di guida, elaborate da istituti nazionali e sovranazionali, attraverso conferenze e convenzioni internazionali, si è percorso un primo tratto del cammino rivolto a realizzare un compiuto sistema di regole.

Altri hanno fatto cenno a due fondamentali linee di metodo: la via europea e la via americana. I due itinerari non sono divergenti, ma sul punto della individuazione degli obiettivi si integrano, mirando a convergere verso una soluzione ad ampia latitudine.

Quanto alla via europea, un tratto centrale è rappresentato dal Libro Verde della Commissione europea del settembre '95, il quale ha attribuito alla tutela dei diritti d'autore e dei diritti connessi un valore fondamentale sotto tre profili.

Prima di tutto viene in rilievo la dimensione culturale, poiché la protezione della proprietà intellettuale è un elemento trainante e sollecita i soggetti alla creazione di prodotti e di servizi chiamati a circolare sulle autostrade dell'informazione.

Poi si evidenzia la dimensione economica, poiché la tutela effettiva di tali diritti può incoraggiare gli investimenti necessari alla competitività delle industrie culturali e dei commerci dei beni immateriali.

Infine, prende risalto la dimensione sociale, poiché i Paesi ad avanzato sviluppo si orientano, in maniera sempre più accentuata, verso attività e servizi a forte valore aggiunto, grazie alla applicazione delle tecnologie, del *know how* e della creatività; quindi le idee innovative sono in grado di tradursi in nuovi prodotti e in processi generatori, a loro volta, di nuovi posti di lavoro.

Il documento comunitario - e questo è un elemento qualificante - non manca di portare lo sguardo oltre la linea di orizzonte dell'Europa, sottolineando il carattere globale e universale delle questioni considerate, auspicando il proseguimento delle varie iniziative nazionali e internazionali, anche nel quadro della Organizzazione mondiale della proprietà intellettuale. E dando risalto (ecco l'anello di congiunzione tra la via europea e la via americana) al gruppo di lavoro, istituito già nel 1995 dal Presidente Clinton, e incaricato di studiare e applicare la politica del governo americano in materia di proprietà intellettuale e di informazione.

Dai principi enunciati dal Libro Verde trae fonte dapprima la direttiva del Parlamento Europeo del marzo '96, per cui sono tutelate dal diritto di autore le banche dati, che per la scelta e la disposizione del materiale costituiscono opere dell'ingegno proprie del loro autore.

Poi, con una visuale ancora più ampia, è venuta in rilievo nel gennaio 1998 la direttiva europea sulla armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione.

La direttiva si basa sul rilievo che la protezione della proprietà intellettuale stimola lo sviluppo di nuovi prodotti e servizi, nonché l'utilizzazione del loro contenuto creativo.

Ai principi segnati dalle istituzioni europee, si raccorda la posizione dell'Italia, la quale è stata finora il primo Paese dell'Unione Europea ad avere recepito, in una apposita norma, l'esigenza di modulare la protezione dei dati personali in relazione ai servizi di comunicazione e di formazione per via telematica.

Come è noto, la legge base (la legge italiana che introduce nel nostro ordinamento la tutela della riservatezza) prevede norme integrative che verranno emanate in un provvedimento delegato o in una pluralità di provvedimenti delegati. E nel novero di questi provvedimenti delegati rientra anche l'emanazione di un provvedimento che, tra l'altro potrebbe

interessare il flusso di dati in Internet che anche in Italia coinvolge un crescente numero di individui e di imprese.

Dopo aver dato uno sguardo rapido all'itinerario europeo, facciamo un rapido cenno all'altro fondamentale, importante itinerario, quella che potremmo definire la via americana, anche se, come ho detto, varia il metodo dell'uno e dell'altro itinerario, però gli obiettivi sono comuni, sono fondamentalmente condivisi.

Nell'itinerario americano appare bene in risalto il problema di ricollocare i diritti di autore nel quadro della società dell'informazione globale e, particolarmente, nell'ambito di Internet.

La tesi prevalente è che i diritti sui beni immateriali non possono più rimanere legati al principio di territorialità, il quale esprime una concezione statocentrica del diritto, cresciuta in un'epoca segnata da culture nazionalistiche e largamente antecedente all'avanzamento tecnologico della società dell'informazione globale.

Conviene fare richiamo al documento programmatico concernente il commercio elettronico globale, elaborato nel luglio '97 dalla Casa Bianca, al fine di tracciare le linee di guida dell'intervento statunitense. In esso si osserva che lo svolgimento di attività commerciali su Internet comporta frequentemente la vendita e la concessione di diritti sull'utilizzo della proprietà intellettuale.

Ma, per fare tali attività (e parafraso il documento) chi vende deve sapere che la proprietà intellettuale non deve essere negoziata in maniera illecita e gli acquirenti devono essere certi della autenticità dei prodotti acquistati.

Di notevole valore poi è l'affermazione che, in riferimento ai due trattati dell'Organizzazione mondiale della proprietà intellettuale, il governo degli Stati Uniti riconosce l'importanza di delineati standard nazionali e internazionali.

Una particolare attenzione il documento riserva al problema dei marchi di fabbrica e dei nomi di dominio (anche questo è uno dei temi più delicati da affrontare). Sempre parafrasando il documento: nel rilevare che i contrasti finora insorti tra i diritti relativi ai marchi di fabbrica e i nomi di dominio sono stati risolti finora tra le parti in sede negoziale o giudiziale, il documento propone di individuare un regime di autodisciplina, in grado di gestire su base globale il conflitto di interessi.

Non possiamo non sottolineare la importanza di questo orientamento, che, nel settore di cui ci occupiamo come in tanti altri settori della società civile, punta sulle forme di autodisciplina, di autoregolamentazione (anziché sull'intervento autoritativo del legislatore), quali strumenti privilegiati per indirizzare i rapporti economico-sociali.

Un ulteriore profilo: di notevole importanza sono anche gli altri principi enunciati nel documento, per cui gli americani (sono le frasi del documento) "tengono in massima considerazione la privacy collegandola al concetto di libertà e di benessere della persona".

È importante anche l'affermazione che conferma il confluire della via americana e di quella europea verso obiettivi comuni, laddove il documento della Casa Bianca osserva: gli Stati Uniti intendono proseguire nell'analisi delle politiche da adottare, in modo da migliorare la conoscenza dell'approccio degli Stati Uniti alla privacy e garantire che i criteri utiliz-

zati dall'Unione Europea e dalla Commissione Europea nel valutare l'adeguatezza dei livelli di protezione siano in rispondenza anche dell'approccio seguito dagli Stati Uniti. L'Amministrazione Clinton ha rivolto un pressante invito al mondo imprenditoriale per la predisposizione di codici deontologici, finalizzati all'adeguata tutela della riservatezza dei consumatori.

Il governo americano è quindi consapevole che una grande rete comunicativa non può rimanere come un crocevia privo di semafori.

In relazione alle linee suindicate, è da ritenere che la convergenza sostanziale dei due grandi itinerari - la via europea e quella americana - valga a costituire le basi per introdurre una disciplina universalmente accettata di tutela della proprietà intellettuale e della privacy.

È stato rilevato, in un documento della Conferenza ministeriale di Bonn del luglio '97, che le nuove opportunità, recate dalle reti informative globali, comportano anche nuove sfide, in relazione all'esigenza di porre regole adeguate sia di carattere tecnologico che giuridico. Occorre costruire fiducia in tale settore, garantendo il rispetto dei diritti fondamentali della persona e tutelando gli interessi della società in genere, compresi i produttori e i consumatori, particolarmente attraverso un'offerta di servizi equa e trasparente.

È interesse di tutti i Paesi dare risposta a tali sfide, in modo che le reti informative globali contribuiscano a elevare la qualità della vita e a promuovere il ruolo attivo dei cittadini nel processo di sviluppo democratico.

Ed ora diamo la parola all'on. Vincenzo Vita, Sottosegretario al Ministero delle Comunicazioni.

On. Giuseppe Vita

Sottosegretario al Ministero delle Telecomunicazioni

Voglio ringraziare l'Autorità Garante per la protezione dei dati personali, il prof. Rodotà e i membri dell'Autorità per questa iniziativa che consente anche a noi una riflessione su un dibattito che è in corso a livello mondiale. È anche grazie ad iniziative come questa che l'Italia - come è successo nei giorni passati con l'euro e il raggiungimento pieno della presenza nell'Unione Europea dal punto di vista monetario e speriamo sempre più anche politico - si avvicina a quei flussi più evoluti di dibattito sui temi della comunicazione da cui per troppo tempo è rimasta scollegata. Ringrazio, inoltre, il prof. Santaniello per la sua utile introduzione a una tavola rotonda, che spero possa vedere un contributo pertinente da parte mia, perché come sapete, quando si interviene in un convegno di lavoro, di grande interesse e utilità, come questo sarebbe necessario partecipare fin dall'inizio ai lavori,

onde poter rendere il proprio intervento puntuale ed efficace. Il dibattito in corso, come è noto, è soprattutto incentrato si incentra sulla straordinaria evoluzione di Internet. Si avvicina la nuova stagione di Fast Internet come ha accennato recentemente il Vice Presidente degli Stati Uniti Al Gore, con un discorso che forse in Italia qualcuno avrebbe giudicato dirigista, con eccessi di statalismo, - e dei servizi, in generale, veicolati sulla rete Internet, ma non solo.

Torniamo all'Unione Europea, di cui siamo sempre più parte attiva ed integrante. Le direttive comunitarie che hanno liberalizzato il sistema delle telecomunicazioni sono state finalmente tutte recepite dall'Italia. Le ultime nello scorso settembre - con una corsa contro il tempo per evitare di incorrere in infrazione che, purtroppo, in qualche occasione l'Italia ha dovuto subire, a causa di ritardi, spesso molto antichi. È stata avviata la liberalizzazione degli apparati terminali e delle apparecchiature, si è proseguito con la liberalizzazione dei servizi, delle infrastrutture di trasporto; si sta ora pienamente completando il quadro normativo con processi che sono insieme di liberalizzazione secondo le indicazioni europee, ma anche di aggiornamento del nostro quadro di leggi e di regolamenti di riferimento.

Il Ministero delle Comunicazioni sta adesso cercando di affrontare una seconda fase; dopo il doveroso recepimento delle direttive comunitarie, la messa in cantiere di leggi che non c'erano o il cui iter non si era, comunque, concluso sta, infatti, occupandosi delle grandi politiche delle comunicazioni, delle politiche industriali, della specificazione della nostra politica sul sistema delle reti, con particolare riguardo a Internet, per contribuire a garantire un ambiente sicuro e evoluto a tutte le attività che si svolgono nel nuovo contesto comunicativo.

In Europa, tra l'altro, si sta svolgendo, proprio in queste settimane, una importante riflessione sui temi della convergenza. Mi riferisco, in particolare al Libro Verde dell'Unione Europea, della Commissione, e anche al dibattito interno all'OCSE. La presenza di tanti interlocutori, non solo italiani, che saluto, a questa tavola rotonda, mi stimola a ricordare, non certo per nazionalismo, che i temi oggi trattati dal Libro Verde erano già da qualche anno oggetto dei lavori parlamentari in Italia ed hanno trovato, infine, compiuta disciplina con la legge 249 del luglio '97. Tale legge può costituire senz'altro un importante punto di riferimento, per il ruolo della costituenda Autorità per le garanzie nelle comunicazioni, che sta prendendo l'avvio in questi giorni a seguito dell'approvazione del regolamento di funzionamento.

Si tratta di una Autorità unica - ecco un contributo che stiamo cercando di dare al dibattito sulla convergenza, pur divisa in due commissioni (infrastrutture e reti, servizi e prodotti) - con grandi poteri regolatori, che aiuterà a semplificare il sistema italiano, troppo legificato.

Approfitto di questa occasione, per affrontare un tema di grande attualità. Si tratta della proposta della Commissione europea che ipotizza tre diversi sistemi di regolamentazione del nuovo sistema delle comunicazioni: l'utilizzazione ed eventualmente l'estensione del quadro di riferimento esistente; la creazione di un nuovo quadro di riferimento, per la maggior parte dei servizi on-line e interattivi, che dovrebbe coesistere con quelli già applicati alle attività tradizionali di telecomunicazione e di radiotelevisione; come 3° impegnativa ipotesi, infine, la creazione - cito testualmente il testo del Libro Verde - di un quadro di

riferimento globale che applichi approcci normativi simili ai tre settori.

Noi stiamo contribuendo, dopo un confronto con le forze parlamentari, con le aziende, con gli operatori, al dibattito europeo con una posizione che ci è sembrata originale, - e che, approfittando di questa occasione, vorrei sottoporre alla vostra attenzione, - in quanto utilizza quello che di buono c'è in tutte e tre le opzioni. Certamente, infatti, serve un quadro di riferimento innovativo e coraggioso nel cambiare la cornice normativa, ma che tenga anche conto della non linearità dei processi di convergenza e, quindi, data la necessaria coesistenza per un periodo non breve dei vecchi media con i nuovi media, della impossibilità di eliminare il quadro normativo preesistente. Nello stesso tempo occorre tutelare quella che possiamo chiamare la specificità culturale, tutto ciò che attiene alla veicolazione dei prodotti audiovisivi, culturali che attraversano l'insieme del sistema pur convergente nella tecnologia. Anzi, se potessi dire, parafrasando un bel libro sulla televisione di tanti anni fa di un famoso autore inglese (Television, di Raymond Williams) anche la convergenza, come fu la televisione classica alle origini, è insieme tecnologia e forma culturale. Ciò posto, raccogliamo la sfida della terza opzione collegandola però alle altre due; credo proprio che questo governo, che pone tra i suoi obiettivi quello dell'innovazione e dell'evoluzione moderna del sistema, possa contribuire a declinare la modernità con un di più di democrazia anche nella comunicazione e possa, quindi, accettare questa sfida: una cornice nuova, unitaria, dei grandi punti di riferimento nuovi, che attraversino i vari segmenti, mantenendo delle specificità nel sistema normativo o regolamentare. Uno degli insegnamenti, che abbiamo condiviso nel dibattito europeo, è che occorre utilizzare strumenti più agili, più flessibili, - quindi più regolamenti, meno leggi -.

Vorremmo contribuire a questa discussione, che è molto pertinente e attuale, e fare queste considerazioni anche per ricordarci - accennavo a processi non lineari della convergenza, a una tempistica da governare con attenzione - che dobbiamo estendere anche i nuovi servizi on-line, in generale i nuovi sistemi comunicativi in rete, le normative che regolano l'attività dei media cosiddetti tradizionali in alcuni momenti specifici: penso al presidio dei minori o dei soggetti deboli, penso ai temi come le libertà, il diritto di cronaca, la diffamazione, grandi argomenti che devono veicolare, magari con forme normative un po' diverse, ma devono veicolare con la stessa pienezza di tutela dei diritti anche nei nuovi servizi.

Venendo invece a qualche aspetto che ha più a che fare con questo convegno, credo che sussista il problema della tutela non tanto e solo di alcuni vecchi diritti o intesi tali, quanto la loro estensione nella convergenza. Proprio il caso di Internet rappresenta un paradigma di simile necessità.

Tra l'altro siamo impegnati - mi rivolgo anche ad alcuni operatori che ho visto essere presenti oggi - a portare avanti una nuova politica tariffaria, che dia libero ingresso anche in questo campo a nuove energie, risorse, ad imprese piccole e medie. Abbiamo già fatto e sappiamo con quale fatica, una prima tranche di intesa con il monopolista uscente della telefonia e ci piacerebbe che su questo aspetto della politica tariffaria si potesse fare ancora di più. Su questo fronte è impegnato anche il Parlamento, - la IX Commissione della Camera ha in discussione un disegno di legge sull'argomento, - e ci piacerebbe dare un contributo

all'estensione di Internet e dell'utilizzo delle reti, anche con una nuova politica industriale, una grande politica sulle infrastrutture che è compito del governo portare avanti.

Ma per concludere, vengo a qualche aspetto più specifico. Il tema della sicurezza, ad esempio, è un tema di grande importanza, da non sottovalutare. Se la letteratura di questi anni ha un po' mitizzato la figura degli *hackers* con qualche tinta letteraria, credo che non sia da sottovalutare un argomento che, proprio perché non va sopravvalutato con qualche tentazione alla criminalizzazione o qualche eccesso di zelo, non va trascurato. Generalmente sono le sottovalutazioni che portano ai rigurgiti autoritari. Quando scatta virtualmente un'ora X in cui c'è una reazione bisogna, con sapienza democratica, intervenire su tali temi.

Nella sessione di questa mattina, dai materiali che ho visionato e dalle notizie che ho avuto si è trattato molto ampiamente del problema della *privacy* sotto diversi punti di vista; tra l'altro il Presidente Rodotà da molti anni è sul tema una delle massime autorità, mi permetto di dire a livello mondiale, e proprio i suoi insegnamenti hanno, per molti di noi, rappresentato un punto di riferimento obbligato su questo e su altri argomenti. Credo che in questa sede sia da chiarire che forse nella Costituzione italiana non è definito un diritto generale alla privacy. Tuttavia numerosi articoli tutelano singoli ambiti della vita privata dei cittadini da illegittime intrusioni. Mi riferisco ovviamente alla prima parte della Costituzione, che non è stata oggetto di proposte di revisione. Tra gli altri vorrei ricordare l'art. 13 che tutela la libertà personale, l'art. 14 l'inviolabilità del domicilio, l'art. 15 la segretezza della corrispondenza, l'art. 16 diritto di circolazione, l'art. 17 diritto di riunione; il 18 il diritto di associazione, libertà religiosa, il 19 la libertà religiosa, l'art. 33 la libertà di arte e di scienza. Ed è evidente che nei casi in cui occorre giudicare sulla prevalenza di interessi costituzionali tutelati, ma magari in contrapposizione in ipotesi specifiche, potremo sempre fare ricorso all'art. 2, posto a presidio delle dignità umane. La legge italiana sulla privacy è sicuramente molto avanzata, nella protezione dei diritti della persona. Anzi con i chiarimenti che vi sono stati sul tema del diritto all'informazione, mi pare stia portando ad un punto di sintesi positivo; si tratta certamente di un argomento importante, come è importante il tema della proprietà intellettuale che suppongo essere oggetto della prossima comunicazione.

È evidente che la grande ricchezza della nostra civiltà risiede soprattutto nei contenuti, nell'arricchimento dell'offerta e della produzione comunicativa. Ciò vale a livello globale e, a livello locale, è stato coniato anche questo termine di glocalismo, per dare l'idea di un locale che non è più solo periferia, ma è parte integrante dello sviluppo; credo, infatti, che le diverse esperienze culturali, le differenze del pianeta possono costituire una ricchezza da tutelare.

Quindi, il tema della proprietà intellettuale oggi più di ieri è attuale, perché si tratta di combinare il vecchio diritto della proprietà intellettuale, il copyright, con un nuovo grande diritto che è la tutela delle diversità, delle specificità nella globalizzazione del sistema.

Abbiamo del materiale al riguardo, non partiamo da zero. Penso al rapporto Bangeman in cui si affermava che la protezione della proprietà intellettuale deve essere vista come una nuova sfida della globalizzazione, dei multimedia e deve avere la massima priorità a livello europeo e internazionale. Le considerazioni che al riguardo ha fatto il prof. Santaniello mi sembrano importanti.

Lo sviluppo della società dell'informazione impone un'armonizzazione delle normative internazionali. La stessa Conferenza dei Paesi del G7, tenutasi nel febbraio '95 a Bruxelles, confermò la necessità di tutelare il contenuto creativo diffuso dalle infrastrutture di telecomunicazione e, in quella occasione, i ministri incoraggiarono il proseguimento delle diverse iniziative nazionali (bilaterali, regionali, internazionali) anche nel quadro dell'organizzazione mondiale della proprietà intellettuale.

Non voglio qui ricordare tutte le iniziative adottate dalla stessa OMPI, dall'UNESCO, dall'OCSE, all'interno del GATT, le quattro direttive al riguardo dell'Unione Europea. Vorrei, però, ribadire che la protezione del diritto d'autore è una frontiera fondamentale, proprio per salvaguardare i soggetti forse più importanti, ma al tempo stesso più deboli della società dell'informazione e della convergenza: gli autori, donne e uomini che scrivono i testi, che pensano, che immaginano con fantasia creativa quello che poi si vede, si sente o i dati che corrono, le piccole e medie imprese che non hanno meno diritti dei più grandi gruppi. Tutto ciò a garanzia di quel pluralismo che è alla base della coesistenza civile e della democrazia.

Infine, la comunità internazionale in questi mesi è impegnata nella discussione del grande tema della firma digitale, che costituisce uno strumento fondamentale per garantire l'esercizio dei diritti delle persone; penso, in particolare alla possibilità di interazione con la pubblica amministrazione, alla evoluzione che può esservi in un Paese come il nostro o anche alla possibilità di concludere accordi di tipo commerciale.

Possiamo dire che, grazie all'approvazione del decreto n. 513 del novembre 1997, l'Italia si è posta tra i Paesi all'avanguardia in materia e per questo sicuramente merita anche un plauso l'opera del Ministro della Funzione Pubblica, Franco Bassanini, che sta lavorando con grande assiduità per snellire procedure, attività della pubblica amministrazione, rapporti tra cittadini e pubblica amministrazione.

Infine, il commercio elettronico. Le transazioni economiche trovano sempre più spazio all'interno di Internet, ad esempio. Esse potranno svilupparsi solo se definiremo un quadro regolamentare in grado di offrire certezze e sicurezza a tutti coloro che utilizzano la rete.

E qui riemerge ancora una volta con forza il problema della tutela dei diritti degli utenti, dei consumatori. È evidente che l'acquisto di prodotti pubblicizzati sulla rete presenta nuovi problemi, relativi alla garanzia della qualità degli stessi prodotti, alla sicurezza dei commerci. Con tutto ciò dobbiamo cimentarci in fretta, non c'è tempo, lo sviluppo è veloce.

Aumentano, quindi, e non diminuiscono le nostre responsabilità: le responsabilità del governo, le responsabilità di tutte quante le istituzioni, politiche e amministrative. Noi vogliamo fare la nostra parte. Non ci sottraiamo perché sentiamo che, in questo dibattito e in questo grande passaggio di epoca, si giocano più diritti di cittadinanza delle persone. Ed è una soglia fondamentale, che si può varcare in tanti modi. C'è un modo autoritario, c'è un modo democratico. Noi vorremmo varcare questa soglia in modo democratico, - come ha indicato nella sua relazione il prof. Rodotà, che ha affrontato con chiarezza tanti punti - e credo che il dibattito possa portare, con il contributo di tanti, con una nuova alfabetizzazione elettronica, una nuova formazione, con impegni prioritari anche per noi, a fornire a tutti saperi e strumenti di base per poter entrare nella grande rete senza esserne travolti.

Tutto ciò che si può dire non basta. Non basta mai. Quante volte le iniziative che prendiamo vengono, anche giustamente, criticate dicendo: sì, ma c'è qualche cosa di più.

C'è molto di più. Continuiamo con grande passione, con grande decisione e in tutte le sedi: in Italia, in Europa, a livello internazionale, facciamo qualcosa di più per noi e anche per i Paesi più poveri, poveri anche sotto il profilo dei saperi e non solo sotto quello dell'economia. Anzi, le due cose sempre più si intrecceranno: sperando che la mia comunicazione, voglia suonare anche come un nostro impegno a dare un contributo a un'attività così delicata, vi ringrazio e mi auguro che vi saranno altre occasioni di confronto.

Prof. Giuseppe Santaniello

Ringrazio l'on. Vita per il contributo di completezza, di incisività, di chiarezza. È una relazione che amplia la dimensione, amplia la linea di orizzonte del nostro convegno perché nella analisi svolta dall'on. Vita confluiscono molteplici fattori, positivi e innovativi.

La relazione non tocca soltanto il sistema nella sua attualità, ma soprattutto traccia le linee di sviluppo, le linee di prospettiva per segnare un forte avanzamento culturale e sociale nei settori interconnessi dell'informazione e dei diritti della riservatezza e della tutela della persona umana.

La parola alla prof.ssa Samuelson.

TAILORING COPYRIGHT TO PROMOTE GROWTH OF THE INFORMATION ECONOMY

By. Pamela Samuelson
Professor of Information Management & of Law,
University of California at Berkeley, USA

An important objective of the information infrastructure or information society policy planning initiatives undertaken in the European Union and elsewhere is promoting development of the information economy. With a highly educated and literate citizenry, the EU should be well-positioned to become a net producer of information products and services able to compete successfully in the global information marketplace. It is readily apparent that ensuring an appropriate degree of legal protection for intellectual property is necessary to provide incentives to making investments in the development of computer software, computer databases, multimedia, and other information products and services. Not surprisingly, information society planning initiatives have made protection of intellectual property a high priority of the policy planning process. Equally important to the growth of the information economy, though, is an appropriate degree of protection for personal data because the electronic commerce in information products and services is unlikely to reach its full potential unless there is adequate protection of personal privacy. Growth of the information economy is of particular concern in the EU because in the last decade unemployment has been high and job creation has been low. Stimulating investments and markets in information sectors should bring about new and better-paying jobs for citizens of the EU and enable Europeans to share in the wealth of the global information economy.

If job creation and a vital information economy is the main goal of EU policy planning for the information economy, European policy planners should make changes to the proposed directive on copyright and related rights in the information society. This directive needs to be tailored in a manner that will better promote innovation in European information industries. The draft directive currently under consideration in the EU will do more to enrich and protect the interests of established players in today's copyright industries than to promote innovation and growth of a vital information marketplace in the EU.

A core problem with the proposed European directive on copyright is that it seems to assume that strengthening intellectual property rights will automatically lead to more investment in creation of intellectual works and a more prosperous information economy. This is not so. Recent work by economists who study information and intellectual property demonstrates that just as it is possible -and undesirable- to underprotect intellectual creations which undermine incentives to invest in innovation, it is also possible -and equally undesirable- to overprotect intellectual creations. Unlike physical goods, whose optimal

production can generally best be achieved by very strong property rights, intellectual goods can only be optimally produced where there is a balance between the level of protection granted to a first creator and the availability of breathing space for follow-on creation. Innovation is a dynamic process that can be retarded if first-generation creators have the power to thwart plans of upstart follow-on creators who see opportunities to build on the first comer's work. This insight is important because most innovation is of an ongoing, cumulative sort, building on preexisting works. This is especially true in innovative information technology markets.

This article will explain why the proposed European directive on copyright and related rights in the information society poses serious risks for overprotecting copyrighted works and hindering the EU's objectives for developing its information economy. Among the negative consequences likely to flow from adopting overprotective rules is a likely inhibition of investment in innovative products and services in EU member states that, if made in the EU, would vitalize the European information economy. Adoption of overprotective rules may cause some European investors to send their investments elsewhere, to jurisdictions where the local intellectual property policy is more balanced and thus favorable to the growth of new information businesses. Overprotective intellectual property rules may also contribute to a "brain drain" of the EU's most creative information technology professionals to places, like Silicon Valley, where the law is more hospitable to promoting innovation. As an American who would like to see healthy competition in the creation of new wealth in the global information economy, it saddens me to see EU policymakers on the verge of adopting policies that may disadvantage Europe's information economy in this way.

Section I of this article will explain why the broad grant of a right in copyright owners to control all temporary copies of works, coupled with a very narrow exception to enable temporary copying incidental to use of a work, is likely to chill the innovation and growth in the EU. Section II will explain why the provision to regulate the circumvention of technical protection systems in the proposed directive will also be harmful to innovation in the EU.

I .OVERBROAD RIGHTS AND UNDULY NARROW EXCEPTIONS WILL DETER INNOVATION

Two rights-related provisions of the proposed European directive will negatively interact to impede innovation in European information technology sectors. An overbroad grant of rights appears in Article 2 of the draft directive. It would require member states to confer on authors an exclusive right to authorize or prohibit direct or indirect, temporary or permanent reproductions of protected works by any means or in any form. The unduly narrow exception provision appears in Article 5.1. It provides an exception to the temporary copying provision of Article 2 insofar as temporary copies are incidental to use of a work and have no independent economic significance. Under Article 5.1, no infringement of copyright would occur when the purchaser of a CD-ROM encyclopedia used it in the CD-ROM drive of his computer, an action that inevitably requires the making of tempo-

rary copies of the contents to enable access and viewing of the encyclopedia.

It is curious that the draft copyright directive should contain these provisions given that very similar provisions were soundly rejected at the diplomatic conference convened to consider an international treaty on copyright law held in December 1996 under the auspices of the World Intellectual Property Organization (WIPO). This is partly the result of efforts made by representatives of innovative information technology companies from the US and the EU who attended the WIPO diplomatic conference as nongovernmental observers (NGOs) to explain why an overbroad treaty provision on temporary copying would have a harmful impact on innovation. Some of the opposition to the temporary copying provision of the proposed copyright treaty emanated from representatives from some EU member states, particularly from the Scandinavian countries whose information technology sectors have been growing rapidly. In the end, delegates to the diplomatic conference decided it was premature for a copyright treaty to mandate the regulation of all temporary copies other than those incidental to use of a work.

In view of the fact that the WIPO Copyright Treaty concluded at that diplomatic conference does not contain a provision requiring regulation of temporary or indirect copies, the European Commission cannot explain its proposed Article 2 as necessary to implement the WIPO Copyright Treaty. Nor can it explain its unduly narrow exception to the temporary copying provision as necessary to implement the treaty. An agreed statement of interpretation to the WIPO treaty indicates that nations could "carry forward and appropriately extend into the digital environment exceptions and limitations in their national laws which have been considered acceptable under the Berne Convention." The agreed statement goes on to say that signatories to the treaty can "devise new exceptions and limitations that are appropriate to the digital environment." Perhaps the Commission's intellectual property policymakers have fallen victim to the "more protection = more investment = more innovation" fallacy mentioned above.

To be fair, one must point out that the proposed EC directive would mandate an exception for temporary copies that are integral to a technological process made for the sole purpose of enabling use of a work and that have no independent economic significance. In addition, the proposed directive's recitals indicate that some caching and browsing of works in digital form may be permitted. However, neither of these limitations on the temporary reproduction right allows enough flexibility to enable new uses of works to emerge. The high protectionist strategy embodied in the draft directive proposes a sweeping rule to regulate all temporary copies until and unless very specific kinds of temporary copies that have been excepted.

With all due respect to the Commission, this is not the optimal way to proceed. At a workshop sponsored by the IMPRIMATUR project in Amsterdam last October, one group of representatives from major publishing houses, recording industries, telephone companies, and librarians, among others, reached consensus that it was premature to regulate temporary copies of works in digital form because too little was known yet about what kinds of temporary copies are made in digital information processing systems and which of

them should be regulated and which left alone. The group thought it would be helpful for computer scientists, economists, and lawyers to work together to build a taxonomy of temporary copies to provide a basis upon which sound regulations of temporary copies might be developed.

It may be helpful to illustrate how proposed Article 2 of the directive may inhibit the growth of new information businesses with some examples. Search engine companies, such as Yahoo!, routinely gather data about what information is available at other sites on the web by sending specialized programs, known colloquially as spiders, to visit those sites to gather this information. When the spiders get to a particular World Wide Web site, they make temporary copies of the contents of the site in order to extract information about its contents. The information extracted by a spider program is shipped back to the database relied upon by the search engine so that when a user requests information of a particular type, the user can get information about its availability at particular sites. From the standpoint of users, the beneficial result of this kind of program is that information on the Internet is made more accessible. From the standpoint of the information economy, innovative companies that have developed search engine and spider technology have created a new service with commercial value that may enable businesses, for example, to connect with new customers. Temporary copies are an integral part of the process. These temporary copies are not made for the sole purpose of enabling use of the site, as they would be if they had been made to permit a user to browse the site. It may also be difficult to say they have no independent economic significance, since the owner of content at a particular site might be keen to charge money for temporary copies made to index the site. If the European directive were to make such temporary copies illegal, this would be unfortunate as search engine companies have been an important sector of growth in the emerging information economy on the net. Surely the Commission does not wish to disable European entrepreneurs from partaking in this growth area of the networked economy.

Filtering software products operate in a similar fashion to search engine spiders. To filter digital information, programs must make temporary copies of the information to be filtered. Based on the results of this processing, certain content may be made available to the user of the filtering program and other content will be blocked. Filtering software has become particularly useful as a means to protect children against indecent or other undesirable content on the net. Filtering programs, like search engine and spider software, have achieved considerable commercial success in the U.S. Yet they too require processing of temporary copies for purposes other than merely enabling use of the information for the purposes the site owner initially intended. Outlawing the development of filtering software would not be in the best interests of the European Union.

Yet another example of a program that uses other digital data as input to produce a more useful output is a program that allows users to assign sounds to particular kinds of visual information in digital form. At a conference on computer-human interaction sponsored by the Association for Computing Machinery (a computing professionals' association with approximately 80,000 members worldwide) in 1991, I had the opportunity to see a

demonstration of a software tool of this sort. One demonstration involved the reprocessing of a digitized chart (in which it is plausible to assume that someone held a copyright) that depicted the pay scales and seniority of scientists in the US. The demonstrator assigned bass sounds to symbols representing male scientists and piccolo sounds to symbols representing female scientists to help interpret the chart. With the aid of this tool, one could "hear" as well as "see" how few senior well-paid women scientists there were. A tool of this sort also requires the making of temporary copies, as does a system built by a computer scientist friend of mine that used signals emitted by a stereo system as it played a sound recording as input for a laser system. The laser system made temporary copies of the audio signals and transformed them into light patterns that changed in shape as the music changed in rhythm and tone. The laser system software could easily be commercialized.

These are only a few of the hundreds of examples of innovative software systems that have commercial value that involve the temporary reprocessing of data or programs. The robustness of the information economy in Silicon Valley in the U.S. is mainly attributable to the imagination of creative computer scientists and entrepreneurs willing to take the risk to bring these innovations to the marketplace. Another factor that enables this robust development and innovation is an intellectual property system that is more finely tuned in the U.S. than in the E.U. to promoting innovation and the growth of new information technology businesses. U.S. law would not regard the temporary reprocessing required by the innovative programs described above as illegal, in part because there is so much new value and expression that these follow-on creators add to the marketplace. If the EU wishes to grow its information economy, it would do well to tailor its copyright policy in a way that will be friendly to information entrepreneurs.

II.OVERLY RESTRICTIVE REGULATIONS OF CIRCUMVENTION AND INFRINGEMENT-ENABLING TECHNOLOGIES IS HARMFUL TO INNOVATION

Another troublesome provision of the proposed European copyright directive is proposed Article 6.1. It would require member states to outlaw "any activities, including the manufacture or distribution of devices or the provision of services" which have only limited commercially significant purpose or use other than to circumvent "any effective technological measure designed to protect copyright". If the goal of the Commission's policy is to grow Europe's information economy, it is surprising that it would propose a regulation that significant players in Europe's information technology industry, such as Nokia, perceive to be harmful to this industry. The information technology sector should not be sacrificed simply because some established players of the traditional content industries are anxious about digital technologies.

As with proposed Articles 2 and 5.1, the Commission cannot justify proposed Article 6.1 on the ground that its adoption is required by the WIPO Copyright Treaty. While the draft copyright treaty considered at WIPO contained a similar provision to proposed Article 6.1, that proposal too met with substantial opposition at the WIPO diplomatic conference. Opposition arose from concerns that widespread use of technical protection measures, along with strict regulation of circumvention and technologies with circumvention-enabling uses would undermine the ability of the public to make appropriate fair uses of copyrighted works. It also threatened to privatize, or in some cases reprivatize, works

and information that under the law would be in the public domain. The treaty adopted in Geneva requires countries to regulate acts of circumvention when done to enable copyright infringement. It does not require nations to regulate acts of circumvention for other purposes. Nor does it require regulation of so-called circumvention technologies. A proposal to regulate such technologies was rejected by delegates to the WIPO conference in favor of a more limited norm. While the Commission is free to choose to go beyond mere implementation of the treaty, it should be concerned about proposing a norm that will chill investment in innovative information technology products.

To understand why proposed Article 6.1 might inhibit growth of the information economy, it is first necessary to consider whether there are circumstances in which the circumvention of a technological protection measure might be justifiable. This is important because if one views the act of circumventing a technical protection measure as per se unjustifiable, it is much easier to conclude that it is a good idea to regulate technologies which can be used to circumvent such a measure. Conversely, if one regards the act circumvention as justifiable in a fairly large number of situations, then one should be more hesitant to outlaw technologies with circumvention-enabling uses and more inclined to focus one's regulations on the act of circumvention itself when done for illicit rather than licit purposes. Someone who circumvents a technical protection system in order to infringe a copyright should be punished, but someone else who engages in an act of circumvention for a legitimate purpose should be free to do so. In general, countries should be wary of regulating a technology with substantial non-infringing uses.

In the U.S., there has been considerable debate about regulation of the act of circumvention and of technologies having circumvention-enabling uses. To some degree, this debate has pitted the lobbyists of Hollywood against the entrepreneurs of Silicon Valley who have allied themselves with consumer electronics industry groups concerned about the impact on innovation and the market for information technology products that would result from regulations of these sorts. The bill, as initially proposed, favored Hollywood's interests far more than Silicon Valley's, but over time the bill has become more balanced. Silicon Valley and consumer electronics industry groups, for example, were able to persuade the U.S. Congress to put into the WIPO implementation legislation a provision that exempts technology providers from liability if their systems aren't able to process some technical measure that a copyright owner had employed to protect a work. There is thus no duty on the part of equipment manufacturers to build systems capable of "reading" any technical protection system a copyright owner might decide to use. They must merely refrain from making and selling technologies that actively defeat technical protection systems and were designed and sold for this purpose.

But let's return to the subject of justifications that might be offered for circumventing a technical protection system. The bill that was originally introduced into Congress recognized only one justification for circumventing a technical protection system, that which enabled law enforcement and national security authorities to carry out appropriate functions. However, over time, a number of other justifications, several of which have innova-

tion and competition overtones, have been deemed acceptable by one or both of the Congressional houses. Computer and software industry groups, for example, persuaded the Congress that circumvention of a technical protection system for a legitimate purpose such as to decompile a computer program to discern details of the program's interface to enable the development of an interoperable program was justifiable. This comports with E.U. software copyright policy which regards interoperability as important to competition and innovation in the computer software industry. In addition, computer security researchers persuaded the House of Representatives to recognize that it is impossible to do computer security research, especially in the cryptology field, without attempting to circumvent a technical protection system that has been deployed and alleged to be secure. The long term security of computer systems depends on the legality of the act of circumvention when undertaken for legitimate cryptologic purposes, as well as on the legality of cryptology tools to enable computer security researchers to test the security of these systems.

Both houses of the U.S. Congress have also created a "shopping privilege" for nonprofit institutions, so that if they need to defeat a technical protection system in order to view technically protected content to decide whether to buy it or not, they can do so. The House of Representatives has also recognized the legitimacy of defeating technical protection systems if they are interfering with reception of otherwise lawful displays of works, if the technical protection system is intruding on the privacy of individual users (for example, by monitoring what users are reading), or if this is necessary to protect children from indecent materials. In addition, the House of Representatives made it clear that defeating a technical protection system in order to engage in fair use is lawful. This suggests that there will be no change in U.S. copyright law as regards the legality of circumventing a copy-protect feature of computer software in order to make a backup copy of the software. This issue was decided in the U.S. Vault v. Quaid case, in which an appellate court ruled that it was legal for a company to sell software capable of unlocking another company's copy-protect system because the "spoofing" software enabled consumers to make lawful backup copies, and thus, the software had a substantial noninfringing use that justified its distribution in the market.

While Article 6.1 leaves some discretion to member states about how to implement regulations of circumvention and of circumvention-enabling technologies, it does not consider the implications of broad or narrow implementations as regards innovation or other public policies, such as privacy and freedom of expression. If the Commission cares about promoting innovation and growth of new information technology businesses, it ought to be more explicit about how these new forms of regulation should be tailored. Without guidance from the Commission, member states may mistakenly think that the more restrictive their rules are, the better off copyright industries will be.

CONCLUSION

The information society will only prosper if there is a vital information economy. A vital information economy will only thrive where there is a meaningful balance of interests in copyright legislation. The proposed European directive on copyright and related rights in

the information society does not adequately balance interests. It grants unduly broad rights to owners of copyrighted works and the technical protection systems they might employ to reinforce legal protections, and unduly narrow exceptions and limitations on those rights. If the E.U. wants to induce more innovation and investment in creative information technology products and services, it must correct the imbalance in these legal proposals.

Otherwise, the E.U. will end up being a net importer of information products and services from other places, and may lose out in the global competition for information technology jobs and investment. While U.S. firms will gladly take advantage of overly restrictive E.U. rules, it would be best for the global information economy if European developers could compete on a level playing field with U.S. firms. This is why the European Parliament should adopt more balanced rules for copyright and related rights in the information society.

ADATTARE LA NORMATIVA SUL DIRITTO D'AUTORE PER PROMUOVERE LO SVILUPPO DELL'ECONOMIA DELL'INFORMAZIONE

By. Pamela Samuelson
Professor of Information Management & of Law, University of California at Berkeley, USA

Un obiettivo importante delle iniziative intraprese nell'Unione Europea ed in altre sedi per elaborare una politica delle infrastrutture informatiche o della società dell'informazione è rappresentato dalla promozione dello sviluppo dell'economia dell'informazione. I cittadini dell'UE hanno un livello elevato di istruzione ed alfabetizzazione, e ciò dovrebbe garantire all'UE un buon punto di partenza per divenire un produttore di prodotti e servizi dell'informazione in grado di competere con successo nel mercato globale delle informazioni. Risulta immediatamente evidente che occorre garantire un grado adeguato di tutela giuridica della proprietà intellettuale per incentivare gli investimenti nella messa a punto di software, database computerizzati, supporti multimediali ed altri prodotti e servizi dell'informazione. Non stupisce osservare che le iniziative legate alla pianificazione della società dell'informazione hanno considerato prioritaria la tutela della proprietà intellettuale.

Tuttavia, ai fini dello sviluppo dell'economia dell'informazione assume pari importanza una tutela adeguata dei dati personali, poiché è improbabile che il commercio elettronico di prodotti e servizi dell'informazione esprima appieno le sue potenzialità in assenza di una protezione adeguata della privacy. Lo sviluppo dell'economia dell'informazione riveste particolare interesse per l'UE, poiché nell'ultimo decennio il tasso di disoccupazione si è mantenuto elevato e sono stati creati pochi posti di lavoro. Attraverso la promozione degli investimenti e dei mercati nei settori dell'informazione dovrebbe essere possibile la realizza-

zione di nuove e più redditizie attività economiche per i cittadini dell'UE, permettendo agli europei di prendersi una fetta della ricchezza associata all'economia globale dell'informazione.

Se la creazione di posti di lavoro e la vitalità dell'economia dell'informazione costituiscono gli obiettivi primari della politica dell'UE nel settore, i politici europei dovrebbero modificare la proposta di direttiva sul diritto d'autore e diritti connessi nella società dell'informazione. Questa direttiva deve essere modificata in modo da favorire in misura maggiore l'innovazione nel settore a livello europeo. La proposta di direttiva attualmente all'esame dell'UE contribuirà ad arricchire e tutelare gli interessi dei soggetti che già partecipano stabilmente alle attività legate al diritto d'autore, più che a promuovere innovazione e sviluppo di un mercato vitale delle informazioni a livello UE.

Un problema di base della proposta di direttiva europea sul diritto d'autore è che essa sembra presumere che potenziando i diritti legati alla proprietà intellettuale si otterrà automaticamente un aumento degli investimenti per la creazione di opere dell'ingegno e migliorerà lo stato dell'economia dell'informazione. Le cose però non stanno così. Studi recenti condotti da economisti in materia di informazione e proprietà intellettuale dimostrano che così come è possibile - e non auspicabile - un approccio riduttivo alla tutela delle opere dell'ingegno, poiché ciò elimina gli incentivi ad investire in innovazione, è parimenti possibile, ed egualmente non auspicabile, un approccio iperprotettivo nei confronti delle opere dell'ingegno. A differenza dei beni fisici, la cui produzione ottimale è resa possibile soprattutto attraverso diritti proprietari forti e ben definiti, una produzione ottimale di beni intellettuali si può avere solo se esiste un equilibrio fra il livello di tutela riconosciuto al primo inventore e la disponibilità di uno spazio di manovra per eventuali successive invenzioni. Innovare è un processo dinamico che può venire rallentato se gli inventori di prima generazione hanno la possibilità di schiacciare l'attività di inventori successivi che intravedono la possibilità di sfruttare l'opera del primo inventore. Si tratta di un punto importante, poiché l'innovazione costituisce in gran parte un processo in fieri, cumulativo, fondato su opere preesistenti. E tutto ciò vale in modo particolare per i mercati delle tecnologie innovative dell'informazione.

Nella mia presentazione cercherò di illustrare per quale motivo la proposta di direttiva sul diritto d'autore e diritti connessi nella società dell'informazione comporti gravi rischi di iperprotezione nei confronti delle opere tutelate dal diritto d'autore e possa ostacolare il raggiungimento degli obiettivi posti dall'UE ai fini dello sviluppo dell'economia dell'informazione. Fra le probabili conseguenze negative derivanti dall'adozione di norme protezionistiche va menzionata l'inibizione degli investimenti in prodotti e servizi innovativi negli Stati membri dell'UE, che potrebbe invece rivitalizzare l'economia dell'informazione in Europa. L'adozione di norme iperprotettive può spingere gli investitori europei a rivolgersi altrove, verso paesi ove la normativa in materia di proprietà intellettuale è più equilibrata e quindi più favorevole allo sviluppo di nuove attività imprenditoriali nel settore dell'informazione. Inoltre, l'introduzione di norme eccessivamente protettive nei confronti della proprietà intellettuale può contribuire ad un vero e proprio "drenaggio di cervelli", per cui i migliori specialisti nel campo delle tecnologie dell'informazione potrebbero lasciare

l'Europa per altri lidi - come Silicon Valley, dove esistono norme di legge meglio in grado di favorire l'innovazione. Da cittadina americana cui farebbe piacere assistere ad una sana competizione nella creazione di nuovo benessere entro l'economia globale dell'informazione, mi rattrista vedere che i politici dell'UE stanno per fare scelte che possono svantaggiare l'economia europea dell'informazione.

Nella prima parte cercherò di spiegare per quale motivo il riconoscimento ai titolari di diritti d'autore di un diritto eccessivamente esteso di controllare tutte le copie temporanee di un'opera, unito alla previsione di eccezioni molto limitate per quanto riguarda l'effettuazione di copie temporanee incidentali all'utilizzo di un'opera, rischi di congelare innovazione e sviluppo nell'UE. Nella seconda parte illustrerò i motivi per cui anche la disposizione contenuta nella proposta di direttiva, mirante a regolamentare l'aggiramento di sistemi tecnici di protezione, risulterà egualmente dannosa per l'innovazione nell'UE.

I. DIRITTI ECCESSIVAMENTE AMPI ED ECCEZIONI INOPPORTUNAMENTE LIMITATE SCORAGGERANNO LE INNOVAZIONI

Due disposizioni in materia di diritti contenute della proposta di direttiva interagiranno in modo negativo, impedendo le innovazioni nel settore della tecnologia dell'informazione a livello europeo. Il riconoscimento di diritti eccessivi appare previsto nell'art. 2 della proposta di direttiva. Esso impone agli Stati membri di riconoscere agli autori un diritto esclusivo di autorizzare o vietare la riproduzione diretta o indiretta, temporanea o permanente, con qualunque mezzo e in qualunque forma, di opere protette. L'art. 5.1 stabilisce invece l'eccezione inopportunamente limitata di cui si diceva: esso prevede infatti un'eccezione alla disposizione sulla copia temporanea di cui all'art. 2 nella misura in cui le copie temporanee siano incidentali all'utilizzo di un'opera e non abbiano alcuna valenza economica indipendente. In base all'art. 5.1., non si configurerebbe violazione del diritto d'autore se l'acquirente di un'enciclopedia su CD-ROM la utilizzasse nel lettore di CD del proprio computer - un'azione che inevitabilmente richiede l'esecuzione di copie temporanee del contenuto per consentire di accedere all'enciclopedia e visualizzarne il testo.

È curioso osservare che la proposta di direttiva contenga le disposizioni di cui sopra, quando disposizioni molto simili furono sonoramente respinte durante la conferenza diplomatica convocata per discutere di un trattato internazionale sul diritto d'autore tenutasi nel dicembre 1996 sotto l'egida dell'OMPI (Organizzazione mondiale della proprietà intellettuale). A tale risultato si giunse anche grazie all'impegno dei rappresentanti di società operanti nel campo dell'IT negli USA e nell'UE, i quali parteciparono alla conferenza diplomatica dell'OMPI a titolo di osservatori non governativi (ONG) per spiegare i motivi per cui una disposizione del trattato eccessivamente ampia in materia di copie temporanee avrebbe influito negativamente sull'innovazione nel settore. Alla disposizione sulle copie temporanee contenuta nella proposta di trattato sul diritto d'autore si opponevano anche i rappresentanti di alcuni Stati membri dell'UE, in particolare quelli dei paesi scandinavi dove si è

avuto un rapido sviluppo dei settori legati alle tecnologie dell'informazione. I delegati presenti alla Conferenza diplomatica stabilirono in ultimo che era prematuro imporre attraverso un trattato sul diritto d'autore la regolamentazione di tutte le copie temporanee diverse da quelle incidentali all'utilizzo di un'opera.

Alla luce del fatto che il Trattato OMPI sul diritto d'autore concluso durante la conferenza diplomatica di cui sopra non contiene una disposizione che prevede la regolamentazione delle copie temporanee o indirette, la Commissione europea non può motivare la proposta relativa all'art. 2 con il fatto che quest'ultimo è necessario per dare attuazione al trattato OMPI sul diritto d'autore. Nè può motivare l'eccezione limitata alla disposizione sulle copie temporanee in quanto necessaria a dare attuazione al trattato stesso. In una dichiarazione interpretativa concordata relativa al trattato OMPI si afferma che le nazioni "potrebbero trasferire all'ambiente digitale ed ampliare opportunamente eccezioni e limiti previsti dalla legislazione nazionale e giudicati accettabili ai sensi della Convenzione di Berna". Nella dichiarazione si prosegue affermando che i soggetti firmatari del trattato possono "individuare nuove eccezioni e nuovi limiti che siano consoni all'ambiente digitale". Forse i responsabili delle politiche della Commissione in materia di proprietà intellettuale sono stati tratti in inganno dall'erronea equazione di cui prima si parlava - ossia "più protezione = più investimenti = più innovazione".

In verità, bisogna sottolineare che la proposta di direttiva CE prevede un'eccezione per le copie temporanee che formano parte integrante di una procedura tecnica attuata per il solo scopo di consentire l'utilizzo di un'opera, e sono prive di valenza economica indipendente. Inoltre, dal preambolo alla proposta di direttiva si evince che è consentita una qualche forma di memorizzazione transitoria e visualizzazione di opere digitali. Tuttavia, nessuna di tali limitazioni del diritto di riproduzione temporanea permette una flessibilità sufficiente a consentire l'emergere di nuovi utilizzi delle opere. L'approccio iperprotezionista adottato nella proposta di direttiva prevede una regolamentazione generale di tutte le copie temporanee con la sola eccezione di alcune tipologie ben individuate di copie temporanee.

Con tutto il rispetto per la Commissione, non si tratta di un approccio ottimale. Durante un seminario promosso dal progetto IMPRIMATUR ad Amsterdam, nell'ottobre scorso, un gruppo di rappresentanti di grandi case editrici, imprese di registrazione, società telefoniche e biblioteche concordava sul fatto che fosse prematuro introdurre norme sulle copie temporanee di opere in formato digitale, poiché ben poco è noto finora sulla tipologia delle copie temporanee eseguite nei sistemi di elaborazione delle informazioni digitali e non sappiamo quali di tali copie debbano essere regolamentate e quali no. Il gruppo riteneva che sarebbe stato utile ricercare la collaborazione fra informatici, economisti ed esperti di diritto in modo da elaborare una tassonomia delle copie temporanee - utilizzabile quale riferimento per regolamentare in modo razionale le copie temporanee.

Può essere utile illustrare con alcuni esempi in che modo l'art. 2 della direttiva, nella sua formulazione attuale, rischi di inibire lo sviluppo di nuove attività nel settore dell'informazione. Le società che gestiscono motori di ricerca, come Yahoo!, raccolgono su base routinaria dati relativi alle informazioni disponibili presso altri siti web, attraverso l'invio di

programmi specializzati (detti comunemente "ragni") verso tali siti in modo da raccogliere le informazioni di cui si diceva. Quando i ragni arrivano su uno specifico sito web, fanno una copia temporanea dei contenuti del sito così da estrarre le informazioni relative al contenuto stesso. Le informazioni estratte vengono ritrasmesse alla base di dati utilizzata dal motore di ricerca, in modo da permettere all'utente che desideri una specifica informazione di sapere se essa sia disponibile presso determinati siti. Dal punto di vista degli utenti, il vantaggio di questi programmi è di aumentare l'accessibilità delle informazioni presenti su Internet. Dal punto di vista dell'economia dell'informazione, le società innovative che hanno messo a punto la tecnologia alla base dei programmi "ragno" e dei motori di ricerca hanno creato un nuovo servizio dotato di valore commerciale e in grado di consentire alle imprese, ad esempio, di contattare nuovi clienti. L'esecuzione di copie temporanee fa parte integrante della procedura. Queste copie temporanee non vengono eseguite al solo scopo di consentire l'utilizzo del sito, come avverrebbe se la loro esecuzione servisse a permettere all'utente di scorrere i contenuti del sito. Non è neppure detto che siano prive di valenza economica indipendente, dato che il proprietario dei contenuti ospitati su un certo sito potrebbe essere intenzionato a far pagare una somma per le copie temporanee eseguite al fine di indicizzare quel sito. Sarebbe un peccato se la direttiva europea dovesse vietare tali copie temporanee, in quanto le società di gestione dei siti di ricerca hanno rappresentato uno dei principali settori in espansione nell'economia dell'informazione emergente sulla rete. Certo la Commissione non desidera togliere agli imprenditori europei la possibilità di partecipare a questo settore in crescita dell'economia in rete.

I prodotti software di filtro operano in modo analogo ai "ragni" dei motori di ricerca. Per filtrare le informazioni digitali occorre prima fare una copia temporanea delle informazioni stesse. In base ai risultati dell'elaborazione eseguita da questi programmi, determinati contenuti verranno resi disponibili all'utente ed altri saranno invece bloccati. I programmi di filtro si sono dimostrati di particolare utilità per proteggere i minori da contenuti osceni o comunque indesiderati presenti sulla rete. Analogamente al software dei motori di ricerca e dei "ragni", questi programmi hanno avuto un notevole successo commerciale negli USA; tuttavia, anch'essi richiedono il trattamento di copie temporanee per scopi diversi dalla semplice possibilità di utilizzare le informazioni per i fini inizialmente previsti dal proprietario del sito. Proibire la messa a punto di software di filtro non sarebbe nell'interesse dell'Unione Europea.

Un altro esempio di programma che utilizza altri dati digitali come input per generare un output più utile è rappresentato da un programma che permette agli utenti di assegnare suoni a determinati tipi di informazioni visive in formato digitale. Durante una conferenza sull'interazione uomo-computer promossa nel 1991 dalla Association for Computer Machinery (un'associazione di professionisti dell'informatica che ha circa 80.000 soci in tutto il mondo) ho avuto la possibilità di assistere alla dimostrazione di un'applicazione software di questo tipo. Si trattava della rielaborazione di un grafico digitale (del quale si può presumere che qualcuno detenesse i diritti d'autore) che mostrava i livelli di reddito e di carriera di scienziati statunitensi. Nella dimostrazione cui ho assistito personalmente

veniva assegnato il suono di un flauto dolce ai simboli che rappresentavano le scienziate, e il suono di un contrabbasso ai simboli corrispondenti agli scienziati, per facilitare l'interpretazione del grafico. Attraverso tale applicazione, si poteva "sentire", oltre che "vedere", quanto poche fossero le donne scienziato che occupavano posizioni elevate e godevano di un salario adeguato. Anche questo programma comporta l'esecuzione di copie temporanee, e lo stesso dicasi per un sistema messo a punto da un mio amico informatico in cui si utilizzavano come input per un sistema laser i segnali emessi da uno stereo durante la riproduzione di un brano musicale. Il sistema laser faceva copie temporanee dei segnali audio e li trasformava in tracciati luminosi che mutavano forma con il mutare del ritmo e del tono della musica. Il software del sistema laser potrebbe essere commercializzato con facilità.

Si tratta solo di alcuni fra le centinaia di esempi di sistemi software innovativi dotati di valore commerciale che comportano la rielaborazione temporanea di dati o programmi. La solidità dell'economia dell'informazione a Silicon Valley negli USA può essere attribuita in gran parte all'immaginazione di informatici creativi e di imprenditori disposti ad assumersi il rischio di commercializzare queste innovazioni. Un altro fattore che permette questo livello elevato di sviluppo ed innovazione è un sistema di tutela della proprietà intellettuale che negli USA è più adatto a promuovere innovazione e sviluppo delle nuove attività nel settore delle tecnologie dell'informazione. In base alla legislazione statunitense, non sarebbe illecita la rielaborazione temporanea resa necessaria dai programmi innovativi sopra descritti, anche perché sono veramente alti il valore aggiunto e le possibilità di espressione che questi inventori di seconda generazione apportano al mercato. Se l'UE desidera far crescere l'economia dell'informazione, sarebbe opportuno che modificasse la propria politica in materia di diritto d'autore in modo da favorire gli imprenditori dell'informazione.

II. UNA REGOLAMENTAZIONE IPERRESTRITTIVA DELLE TECNOLOGIE DI AGGIRAMENTO E VIOLAZIONE È DANNOSA AI FINI DELL'INNOVAZIONE

Un'altra disposizione problematica contenuta nella proposta di direttiva sul diritto d'autore è l'articolo 6(1). Quest'ultimo imporrebbe agli Stati membri di vietare "ogni attività, compresa la fabbricazione o distribuzione di strumenti o la fornitura di servizi che abbiano limitate finalità o utilizzazioni di rilevanza commerciale diverse dall'aggiramento.... di misure tecniche efficaci finalizzate alla tutela del diritto d'autore...". Se la politica adottata dalla Commissione mira a far crescere l'economia europea dell'informazione, è sorprendente che si proponga una norma che soggetti importanti nel settore delle tecnologie dell'informazione a livello europeo (come Nokia) considerano dannosa per le proprie attività.

Non si dovrebbero sacrificare gli interessi del settore delle tecnologie dell'informazione solo perché soggetti ormai affermati nei settori più tradizionali hanno timore delle tecnologie digitali.

Analogamente agli articoli 2 e 5(1), la Commissione non può giustificare la proposta dell'articolo 6(1) adducendone la necessità per dare attuazione al Trattato OMPI sul diritto d'autore. È vero che la proposta di trattato sul diritto d'autore esaminata in sede OMPI

conteneva una disposizione simile a quella dell'art. 6(1), ma anche tale proposta incontrò una forte opposizione durante la conferenza diplomatica OMPI. L'opposizione in questo caso nasceva dal timore che il ricorso su larga scala a misure tecniche di protezione, unita ad una rigida regolamentazione dei casi di aggiramento e delle tecnologie applicabili a tale scopo avrebbe compromesso la possibilità per il pubblico di utilizzare in modo adeguato e leale opere tutelate dal diritto d'autore. La disposizione rischiava inoltre di privatizzare, o riprivatizzare in taluni casi, opere ed informazioni che ai sensi di legge sarebbero di dominio pubblico. Il trattato adottato a Ginevra impone agli Stati di regolamentare gli atti di aggiramento compiuti per permettere una violazione delle norme sul diritto d'autore; esso però non impone agli Stati di regolamentare tali atti quando essi siano compiuti per altri scopi, né di regolamentare le cosiddette tecniche di aggiramento. Una proposta avanzata in tal senso venne respinta dai delegati alla Conferenza OMPI a favore di una norma di portata più ristretta. La Commissione è senz'altro libera di scegliere di andare oltre una semplice attuazione del Trattato, ma dovrebbe chiedersi se sia opportuno proporre una regolamentazione che congelerà gli investimenti in prodotti innovativi delle tecnologie dell'informazione.

Per comprendere i motivi per cui l'art. 6(1) rischia di inibire lo sviluppo dell'economia dell'informazione, occorre prima esaminare se esistano situazioni nelle quali sia giustificabile l'aggiramento di una misura tecnica di protezione. Si tratta di un punto importante, poiché se si considera di per sé inammissibile l'atto di aggirare una misura tecnica di protezione, è molto più facile giungere alla conclusione che sia opportuno regolamentare le tecnologie utilizzabili per aggirare tali misure. Viceversa, se si ritiene che l'aggiramento sia ammissibile in un numero piuttosto ampio di casi, allora si dovrebbe usare maggiore cautela nel bandire tecnologie utilizzabili a fini di aggiramento, preferendo semmai concentrare la regolamentazione sull'atto di aggiramento in quanto tale se compiuto per scopi illeciti anziché leciti. È opportuno punire chi aggira un sistema tecnico di protezione per violare il diritto d'autore, ma chi intraprende un'azione di aggiramento per scopi legittimi dovrebbe essere libero di farlo. In linea di massima, gli Stati dovrebbero guardarsi dal regolamentare tecnologie che trovano consistente impiego per scopi non illegittimi.

Negli USA si è dibattuto a lungo sulla regolamentazione dell'atto di aggiramento e delle tecnologie utilizzabili per scopi di aggiramento. Il dibattito ha visto la contrapposizione, in una certa misura, fra i lobbisti di Hollywood e gli imprenditori di Silicon Valley, che si sono alleati con gruppi dell'industria dei beni elettronici di consumo preoccupati dell'impatto di norme del genere descritto sull'innovazione e il mercato dei prodotti delle tecnologie dell'informazione. Il disegno di legge inizialmente era di gran lunga più favorevole agli interessi di Hollywood che a quelli di Silicon Valley, ma col tempo ha raggiunto una formulazione più equilibrata. Ad esempio, i rappresentanti di Silicon Valley e dell'industria dei beni elettronici di consumo sono riusciti a convincere il Congresso ad inserire nella legislazione da emanare in attuazione del Trattato OMPI una disposizione che esonera da ogni responsabilità i fornitori di tecnologie se i sistemi da questi ultimi prodotti non sono in grado di trattare misure tecniche utilizzate da un titolare di diritti d'autore per proteggere la propria opera. Non esiste pertanto alcun obbligo da parte dei produttori di apparecchiature

di costruire sistemi in grado di "leggere" qualsiasi sistema tecnico di protezione eventualmente utilizzabile dai titolari di diritti d'autore. Essi devono soltanto astenersi dal produrre e vendere tecnologie in grado di neutralizzare sistemi tecnici di protezione che siano state progettate e vendute appositamente per tale scopo.

Torniamo però al tema delle motivazioni che possono essere addotte per giustificare l'aggiramento di un sistema tecnico di protezione. Il disegno di legge inizialmente presentato al Congresso ammetteva una sola giustificazione - ossia, qualora l'aggiramento servisse a permettere a rappresentanti delle forze dell'ordine e ad autorità di sicurezza nazionale di svolgere compiti ad essi propri. Tuttavia, col tempo sono state ritenute accettabili da uno o da entrambi i rami del Congresso una serie di altre giustificazioni, molte delle quali avevano risvolti legati ai temi dell'innovazione e della concorrenzialità. Ad esempio, i gruppi dell'industria informatica hanno convinto il Congresso dell'ammissibilità dell'aggiramento di un sistema tecnico di protezione per scopi legittimi quali la decompilazione di un programma al fine di individuare l'interfaccia del programma stesso in modo da consentire la messa a punto di software interfacciabile. Si tratta di un punto conforme alla politica dell'UE in materia di diritti d'autore sul software, nel senso che anche in questo caso l'interfacciabilità viene giudicata importante ai fini della concorrenza e dell'innovazione nel settore dell'industria informatica. Inoltre, ricercatori in materia di sicurezza informatica hanno convinto il Congresso a riconoscere l'impossibilità di fare ricerca nel settore della sicurezza informatica, soprattutto in riferimento alla criptologia, senza tentare l'aggiramento di sistemi tecnici di protezione che si presume essere sicuri. La sicurezza dei sistemi informatici nel lungo periodo dipende dalla legalità dell'atto di aggiramento compiuto per scopi legittimi di natura criptologica, nonché dalla legalità degli strumenti criptologici stessi, al fine di consentire ai ricercatori di testare la sicurezza dei sistemi in oggetto.

I due rami del Congresso hanno inoltre stabilito un "privilegio di acquisto" per gli organismi non lucrativi, in base al quale questi ultimi possono neutralizzare un sistema tecnico di protezione per visualizzare contenuti protetti in modo da decidere se acquistare tali contenuti o meno. La Camera ha inoltre riconosciuto la legittimità della neutralizzazione di sistemi tecnici di protezione se questi ultimi impediscono la visualizzazione (peraltro legittima) di opere tutelate da copyright, se il sistema di protezione viola la privacy di singoli utenti (ad esempio, perché effettua un monitoraggio delle abitudini di lettura degli utenti), oppure se tale neutralizzazione risulta necessaria per tutelare minori da contenuti osceni. Inoltre, la Camera ha affermato la legittimità della neutralizzazione di un sistema tecnico di protezione per dare corso ad un utilizzo corretto; quest'ultimo dato sembra indicare che non vi saranno modifiche alla legislazione statunitense in materia di copyright per quanto riguarda la legittimità dell'aggiramento di un dispositivo anti-copia inserito in un software al fine di eseguire una copia di backup del software stesso. Si tratta di un tema già affrontato nel caso Vault contro Quaid, in cui una corte di appello ha stabilito che era legale la vendita di software in grado di sproteggere un sistema anti-copia messo a punto da un'altra società in quanto il software di "sprotezione" permetteva ai consumatori di eseguire copie legittime di backup, e quindi aveva un impiego importante di natura legittima che ne giu-

stificava la commercializzazione. È vero che l'art. 6(1) lascia agli Stati membri un margine di manovra per quanto riguarda le modalità di attuazione della normativa su aggiramento e tecnologie utilizzabili a tale scopo, ma non tiene conto delle implicazioni di un approccio più o meno restrittivo per l'innovazione o altri aspetti di pubblico interesse - quali privacy e libertà di espressione. Se la Commissione desidera favorire l'innovazione e la crescita di nuove attività nel campo delle tecnologie dell'informazione, dovrebbe pronunciarsi con maggiore chiarezza sulle modalità con cui adattare ai singoli casi queste nuove forme di regolamentazione. In assenza di indicazioni da parte della Commissione, c'è il rischio che gli Stati membri facciano l'errore di credere che quanto più restrittive saranno le norme nazionali, tanto più saranno favorite le attività legate alla normativa sul copyright.

CONCLUSIONI

La società dell'informazione potrà prosperare solo in presenza di un'economia dell'informazione vitale. Un'economia dell'informazione vitale potrà prosperare solo in presenza di un significativo bilanciamento di interessi nella legislazione in materia di diritto d'autore. La proposta di direttiva europea sul diritto d'autore e diritti connessi nella società dell'informazione non permette un bilanciamento adeguato di tali interessi. Essa riconosce diritti eccessivamente ampi ai titolari di opere coperte da copyright ed ai sistemi tecnici di protezione utilizzabili da tali titolari per potenziare la tutela giuridica, mentre prevede eccezioni e limitazioni inopportunamente ridotte ai diritti di cui sopra.

Se l'UE desidera favorire innovazione e investimenti in prodotti e servizi delle tecnologie dell'informazione, è necessario correggere gli squilibri esistenti nella normativa proposta. In caso contrario l'UE finirà per importare prodotti e servizi dell'informazione da altri paesi, e rischia di perdere posti di lavoro ed investimenti nel quadro della concorrenza globale per le tecnologie dell'informazione. Le società statunitensi saranno ben felici di utilizzare a proprio vantaggio norme eccessivamente restrittive adottate dall'UE, ma per l'economia globale dell'informazione sarebbe preferibile una concorrenza allo stesso livello fra europei ed americani in questo settore. È per tale motivo che il Parlamento europeo dovrebbe adottare norme più equilibrate in riferimento al diritto d'autore e ai diritti connessi nella società dell'informazione.

Prof. Santaniello

Ringrazio la prof.ssa Samuelson per l'elevato contributo all'elaborazione del tema. Mi limito a rilevare il pregio caratterizzante di una relazione così accurata. È un'analisi che fonde due fattori: un alto livello concettuale, e un alto livello operativo. È una relazione che dà la misura di come si possano tracciare proficuamente delle linee di guida per una legislazione adeguata e per una protezione tecnologica.

Diamo ora la parola al prof. Oliva.

DISTRIBUTING INTELLECTUAL PROPERTY: A MODEL OF MICROTRANSACTION BASED UPON METADATA AND DIGITAL SIGNATURES

Prof. Maurizio Oliva
Denison University

Abstract

This paper describes the problem of distributing extremely large corpora of information, heterogeneous and of uneven quality, in a distributed digital environment such as the Internet. This paper argues that a transaction based upon metadata and digital signatures is viable. The paper suggests that authors are the ideal candidates for the generation of the description of their work. Metadata should contain all the information to describe the original work. Digitally signed metadata may substitute original objects, in any form of transaction, until the final retrieval by the end user. Metadata should be digitally signed by all the parties involved in a transaction: the author/merchant, the client, the certification authority. A cycle of signatures combined with additional security measures may achieve the desirable level of fault tolerance by a system of transaction devised for payments under five dollar.

Introduction

The problem of distribution of information is defined by three main aspects: identity, organization and security of intellectual property. One way to establish identity is through the combination of hashing algorithms, public key encryption and metadata. The second aspect is the aspect of organization. Organization can be dynamic and rely upon metadata generated at the origin. The third aspect is the aspect of security which involves several levels and encompasses the handling of intellectual property issues.

Where information can be organized

Information can be organized at several point of its journey from the origin to the recipient. It can be organized at the source. It can be organized at the point of storage, and it can be organized at the point of reception. Examples of organization at the point of ori-

gin may be an author that submits an article to a scholarly journal. The author is usually required to submit an abstract, an abstract associated with the bibliographic reference, contains just enough information about the article to allow its automatic management, in a database such as Infotrack or Cite. The Library of Congress Cataloguing-in-Publication Data (LCCPD) represents a hybrid that shows the potential for metadata generation at the origin. The Publisher who generates the LCCPD is not the author, but it substitutes the author under many aspects such as: reformatting the work, fixating the work, replicating the work (printing), mediating the ownership of the work, distributing the work, and determining the price of the work. Since the western concept of intellectual property relies upon fixation of the work, the publisher is in some way, or represents at a larger extent, the author. Examples of organization at the point of distribution can be a library card catalog, the bookseller catalog, the publisher catalog, the bibliography compiled by a professional organization and many others. The experience of the Library of Congress, who deals mostly with analog media, can be summarized with a simple statement: a central organization, no matter how well funded, powerful, and efficient, cannot perform central generation of metadata to the volume reached by the published information at this point in time.

Examples of organization at the point of reception exist, such as: intelligent agents, or more simply, the bookmarks lists that users keep in their browser. An intelligent agent is able to sort through large corpora of text and summarize it, thus allowing its organization from the point of view of the individual.

A metadata label generated by the author

Distribution of discrete information through metadata labels empowers the individual to assume the role of author, owner, merchant concurrently and without intermediation. It also multiplies the number of transactions, by bringing into the retail market much of the intellectual property that was previously traded in bulk through collective systems such as libraries, universities, organizations, and other institutions. Most important, metadata labels would allow the author/merchant to distribute labels instead of objects; the digital work, the original, would be retrieved only after the transaction has been completed.

Distribution of information based on metadata labels generated by the author can effect the following consequences: generating a lesser traffic, increasing control of the owner over the work, enabling a scaleable, distributed, system for the organization of information. A possible example of classification protocol is the Platform for Internet Content Selection (PICS). PICS is a standard for the format of content rating labels. Semantics are separated from the syntax. Many different rating authorities may exist and the choice of which one to use should belong to the final user. All the dictionaries developed by the rating authorities are interoperable thanks to the PICS standard. Provisions are made for unplanned uses including especially: review labels, classification vocabularies, and IP vocabularies. DSig, is a PICS label for making (DesAutels et al. November 11, 1997) digitally

signed, machine-readable assertions about a particular information resource. Among the different ways to uniquely specify a particular key, the hash or fingerprint (ByHash) is the most useful for this model. A DSig label can establish the identity of the good and the owner through a digitally signed description of the digital work. Metadata labels compliant with the PICS standard could be designed; they could include digitally signed metadata.

Otherwise the DSig label could be extended to include all the required metadata.

The hash provides unique correspondence with the original, while the metadata provide a description of the original including: title, medium, link to the original location, intellectual property conditions, pricing, other works by the author, authorization. It is very important to notice that the metadata label offers a possible solution to the problem of permanence. First and foremost the label can be reissued to integrate additional or revised information. Secondly, the link to the original location may point back to a link maintained by the author. Permanence should be based not upon location but upon identity.

Digital format and especially metadata bring us a step further in the definition of identity by eliminating environmental variables that are circumstantial. It is important that classification rely on some standard of semantics. A plurality of standards of semantics may exist, provided that they comply with a unique standard for syntax. Classification, when monopolized by one culture or one organization may produce control over information. A possible solution may rely upon the separation of syntax and semantics, through a protocol that allows interoperability and coexistence of a variety of classification systems: PICS does this (Resnick 1996).

How digital information can be organized

One of the main component of a system of distribution of digital information is a system of organization. Digital information must be organized in an efficient manner, taking into consideration the high volume of published information and its nature of process rather then fixed document. A metadata standard would allow to organize information dynamically, and in a distributed fashion, as opposed to a cataloguing system or to a directory system that would require a central entity to handle the whole volume of information.

The organization of information, should be dynamic and distributed, and it should be based on metadata generated directly by the author. Metadata labels will need to be transferred over the network, collected in dedicated servers, organized in a structure, searched by an engine, and, finally, displayed through a Web interface. The Resource Description Framework (RDF) is a specification, currently being developed by the W3 Consortium (W3C), that addresses the previously mentioned issues (Swick 1998). It is designed to provide an infrastructure to support metadata across many Web-based activities. Sitemaps, content ratings, stream channel definitions, search engine data collection, digital library collections, and distributed authoring are among its applications. Different types of applications will be able to define the metadata semantics that best serve each of them, but a

common syntax will provide the uniform means to interoperate, and exchange metadata between applications and servers. The definition of the property set will be both human-readable and machine-understandable, and XML will provide the transfer syntax. The development of RDF as a metadata framework and as a general knowledge representation syntax was a consequence of the development of the Platform for Internet Content Selection (PICS) (W3C 1998). RDF with digital signatures will be the key to building electronic commerce, collaboration, and other applications. RDF deals both with a model for representing metadata and with a possible syntax for expressing and transporting this metadata. This transport will take place among heterogeneous servers and clients, and RDF will privilege interoperability. RDF, like PICS does not contain predefined vocabularies for authoring metadata. New vocabularies can be designed by anybody. The diffusion of RDF compliant metadata labels will make easier and more precise searching on the Web and automated software agents will also take advantage by collecting information or performing transactions. This mechanism is the result of a joint effort by representatives from many different corporations, and is a very good example of what is commonly defined as an open standard, operating in what is commonly defined as an open system. Once created, the DSig label must be disseminated to large, publicly available collections.

These collections may assume different forms. For the purpose of this paper they will be generally referred to as storage solutions. A storage solution must possess the space to store hundreds of millions of records. It must possess the processing capability to allow directory browsing or engine searches.

How digital information can be distributed

Digital information can be distributed commercially in two main ways: using a physical support or via the network. Distribution of analog and even digital information has long relied upon physical media. This is mainly a consequence of the Western concept of intellectual property reliance upon fixation; fixation privileges embodiment. For the end user it is easier to relate to a CD-ROM as to some property, because of its physical attributes. The CD-ROM support is designed to reproduce some of the characteristics of standard economic goods, and to eliminate some of the characteristics of digital goods: it is difficult to be replicated, and the information contained in it is identified with the physical attributes of the support. A possible model of distribution of information relies on metadata and encryption.

A possible model of microtransaction is based upon three parties: the merchant (who can be the author and owner of the digital work), the client, and the credit company in the form of a payment processing center. The objects involved in the transaction are: the digital work, the metadata label (DSig Label), and the Digital Funds. The system will need the development of at least two applications: a label maker, to be used by the author in association with the application that creates the digital work; and a signature generator to be associated with the mail handler (such as a PGP plug-in for the Web browser). The system is

designed for the handling of very small payments. Because of it, the priority is to limit the overhead imposed by the cost of the transaction. In a system with these characteristics, security can be based upon the trust system. The trust system can be summarized as follows: anybody who is a trusted client of a credit company is trusted until she breaks the trust. Elements of security need to be introduced. In order to identify the signature of the client and the merchant, the credit company may rely upon key escrow or public directories. In order to identify the merchant and the client, the credit company may rely upon its established database of card holders. A further element of security can be limiting the amount of daily and monthly transactions.

Finally confirmation by email can be addressed to the parties of the transaction by the party who closes the transaction (the credit company). Key escrow is a very costly and controversial practice. Its implementation on a global basis is at least very difficult because it infringes upon recognized practices of national jurisdiction. On the other hand, for the purpose of micropayments public directories, combined with posting and expiration dates of the public keys, could provide an economically viable solution. In a distributed environment, such as the Internet, security must be understood in a different way than security in the physical world. The first consideration is that any object is information, and information relevance (existence) tends to zero in absence of communication. Internet security should not prevent copying or other unlawful practices. It should prevent the reposting of material generated through a violation of the law or of a contract between parties. Because it is reiteration that may generate significant economical damage to the merchant/author, not occasional copying. In a certain sense this approach to security can be described as asynchronous as opposed to the type of synchronous security normally applied to transactions. There is no need for establishing a secure channel of two-way communication between the merchant and the client.

The client reads a certified assertion by the merchant and assumes that the identity of the merchant and its assertion are believable, the credit company reads the assertion signed by the merchant and the client as a transaction and verifies the identity of the merchant and the client. Once the merchant receives back its own metadata label, signed by the client and by the credit company, the transaction is complete. Again, it is possible to describe this transaction as an asynchronous transaction, as opposed to the synchronous transaction provided by the Secure Electronic Transaction protocol.

DISTRIBUIRE PROPRIETÀ INTELLETTUALE: UN MODELLO DI MICROTRANSAZIONE BASATO SU METADATI E FIRMA DIGITALE

Maurizio Oliva
Denison University

Abstract

Nel presente testo viene esaminato il problema della distribuzione di corpus di informazioni di grande entità, eterogenee e qualitativamente difformi, in un ambiente digitale distribuito quale Internet. Si afferma la fattibilità di una transazione basata su metadati e firme digitali. L'articolo propone di considerare gli autori come i candidati ideali per generare una descrizione delle rispettive opere. I metadati dovrebbero contenere tutte le informazioni utili a descrivere l'opera originale.

Metadati provvisti di firma digitale possono sostituire gli originali, in qualsiasi transazione, fino al recupero dell'informazione da parte dell'utente finale. I metadati dovrebbero recare la firma digitale di tutti i soggetti che partecipano alla transazione: autore/venditore, cliente, autorità di certificazione. Attraverso un sistema di firme associate ad ulteriori misure di sicurezza è possibile raggiungere il livello desiderato di tolleranza all'errore in un sistema di transazioni progettato per pagamenti inferiori a 5 dollari.

Introduzione

Il problema della distribuzione di informazioni si caratterizza per tre aspetti fondamentali: identità, organizzazione e sicurezza della proprietà intellettuale. Un modo di accertare l'identità consiste nell'associazione di algoritmi di reindirizzamento, crittografia a chiave pubblica e metadati. Il secondo aspetto riguarda l'organizzazione; quest'ultima può essere di tipo dinamico e basarsi su metadati generati all'origine. Il terzo aspetto è quello della sicurezza, e ciò comporta vari livelli e riguarda anche la gestione di tematiche connesse alla proprietà intellettuale.

Dove organizzare l'informazione

Esistono vari momenti nei quali è possibile organizzare informazioni lungo il percorso che dall'origine conduce al destinatario. La si può organizzare alla fonte, oppure nel punto di immagazzinamento, oppure ancora nel punto di ricezione. Un esempio di organizzazione alla fonte è costituito dall'invio di un articolo ad una rivista specializzata da parte dell'autore. L'autore dovrà in genere sottoporre un abstract, ed un abstract associato a riferi-

menti bibliografici contiene per quanto riguarda l'articolo esattamente le informazioni sufficienti a consentirne la gestione automatica in una banca dati tipo Infotrack o Cite. Il sistema di catalogazione della Library of Congress (Library of Congress Cataloging-in-Publication Data - LCCPD) costituisce un ibrido dal quale si evincono le potenzialità della generazione di metadati alla fonte. L'editore dal quale dipende la generazione dell'LCCPD non è l'autore, ma ne fa le veci sotto molti aspetti quali la riformattazione dell'opera, la sua fissazione, la replicazione (stampa), la mediazione sulla proprietà dell'opera, la sua distribuzione e la definizione del prezzo.

Il concetto di proprietà intellettuale in Occidente si basa sulla fissazione dell'opera, per cui l'editore in un certo senso è l'autore, o lo rappresenta in un senso più ampio. Esempi di organizzazione nel punto di distribuzione dell'informazione sono rappresentati da uno schedario biblioteconomico, dai cataloghi di libreria, dai cataloghi delle case editrici, dalla bibliografia compilata da un'organizzazione professionale e da molti altri casi ancora. L'esperienza della Library of Congress, che si occupa in via prevalente di supporti analogici, può essere riassunta in una semplice affermazione:

un'organizzazione centralizzata, per quanto disponga di abbondanti finanziamenti, potere ed efficienza, non può generare metadati in misura pari al volume attualmente raggiunto dalle informazioni disponibili pubblicamente. Dobbiamo infine citare alcuni esempi di organizzazione nel punto di ricezione: è il caso dei cosiddetti "agenti intelligenti", o più semplicemente delle liste di "puntatori" [bookmarks: lett., "segnalibri"] che ogni utente tiene aggiornate nel proprio browser. Un agente intelligente permette di filtrare corpus testuali consistenti generando una sintesi, che ne consente quindi l'organizzazione dal punto di vista del singolo.

Etichette di metadati generate dall'autore

La distribuzione di informazioni discrete attraverso etichette di metadati consente al singolo di assumere contestualmente il ruolo di autore, titolare e venditore, senza intermediazione alcuna. Essa permette inoltre di moltiplicare il numero di transazioni, inserendo sul mercato al dettaglio gran parte della proprietà intellettuale che in precedenza era oggetto di una transazione commerciale in blocco attraverso sistemi collettivi quali biblioteche, università, organizzazioni ed altre istituzioni. Particolare importanza riveste il fatto che le etichette di metadati permetterebbero all'autore/venditore di distribuire etichette anziché oggetti: l'opera digitale, l'originale, verrebbe resa disponibile solo una volta completata la transazione. La distribuzione di informazioni basata su etichette di metadati generate dall'autore può avere come conseguenza una riduzione della mole del traffico, un aumento del controllo esercitato dal titolare sull'opera, la possibilità di creare un sistema scalarizzato e distribuito per l'organizzazione delle informazioni.

Un esempio di protocollo di classificazione è rappresentato dalla Platform for Internet Content Selection (PICS - Piattaforma per la scelta di contenuti su Internet). Si tratta di

uno standard per la formattazione di etichette di giudizio sui contenuti. Gli aspetti semantici sono mantenuti distinti dalla sintassi; possono sussistere più soggetti responsabili della valutazione di giudizio, e la scelta di quello da utilizzare dovrebbe essere appannaggio dell'utente finale. Tutti i dizionari messi a punto dalle autorità di valutazione sono interfacciabili grazie allo standard PICS. È prevista la possibilità di utilizzi non pianificati, in particolare per la creazione di etichette di valutazione, glossari di classificazione, e glossari in materia di trattamento delle informazioni (IP).

L'acronimo Dsig si riferisce ad un'etichetta PICS per la generazione (DesAutels et al, 11 novembre 1997) di enunciati su una specifica fonte di informazioni, corredati di firma digitale e in formato leggibile da macchina. Fra le varie metodiche utilizzabili per specificare in modo univoco una determinata chiave, quella maggiormente utile ai fini del modello proposto è l'algoritmo di riduzione (hash - ByHash). Un'etichetta Dsig è in grado di accertare l'identità dell'oggetto e del proprietario attraverso una descrizione dell'opera digitale corredata di firma digitale. Si potrebbero mettere a punto etichette di metadati conformi allo standard PICS, nelle quali siano inseriti metadati provvisti di firma digitale. Un'altra possibilità sarebbe quella di ampliare l'etichetta Dsig fino a ricomprendervi tutti i metadati necessari.

L'algoritmo di riduzione (hash) garantisce la corrispondenza univoca con l'originale, mentre i metadati forniscono una descrizione dell'originale che comprende titolo, supporto, link con la sede fisica originaria, condizioni della proprietà intellettuale, costi, altre opere dell'autore, autorizzazione. È fondamentale osservare che l'etichetta di metadati offre una possibile soluzione al problema della permanenza. In primo luogo, l'etichetta può essere ricreata in modo da integrare informazioni ulteriori o corrette. In secondo luogo, il link con la sede fisica originale può rinviare ad un link gestito dall'autore. La permanenza dovrebbe basarsi non già sulla sede fisica, bensì sull'identità. Il formato digitale, e in particolare i metadati, ci fanno progredire nella definizione dell'identità eliminando le variabili ambientali, che hanno natura circostanziale.

È essenziale che la classificazione si basi su uno standard semantico; possono esistere più standard semantici, purché siano conformi ad un unico standard di sintassi. La classificazione può condurre al controllo delle informazioni, se diviene monopolio di una sola cultura o di un solo ente. Una soluzione praticabile è data dalla separazione di sintassi e semantica attraverso un protocollo che consenta l'interfacciabilità e la coesistenza di più sistemi di classificazione: e tutto questo è possibile con la PICS (Resnick 1996).

Come organizzare l'informazione digitale

Una delle componenti primarie di un sistema di distribuzione di informazioni digitali è rappresentata da un sistema di organizzazione. L'informazione digitale deve essere organizzata in modo efficiente, tenendo conto della mole di informazioni disponibili pubblicamente e della loro natura di oggetto in divenire più che di documento fissato in forma definitiva. Uno standard basato su metadati permetterebbe di organizzare le informazioni in

modo dinamico e distribuito, rispetto ad un sistema di catalogazione o indicizzazione che necessiterebbe di un ente centrale incaricato di gestire tutto il volume di informazioni.

Queste ultime dovrebbero essere organizzate in modo dinamico e distribuito, sulla base di metadati generati direttamente dall'autore. Sarà necessario trasferire attraverso la rete etichette di metadati, raccogliendole in server dedicati, organizzarle in una struttura, consentirne la ricerca attraverso un motore apposito e, infine, visualizzarle attraverso un'interfaccia Web. La specifica RDF (Resource Description Framework - Infrastruttura per la descrizione di risorse) attualmente in via di definizione da parte del Consorzio W3 (W3C) permette di gestire i problemi sopra indicati (Swick 1998). È pensata per offrire un'infrastruttura che supporti metadati in numerose attività riferite al Web; fra le applicazioni possibili citiamo mappe di siti, giudizi su contenuti, definizione di canali di flusso, raccolta di dati su motori di ricerca, raccolte di biblioteche digitali e gestione distribuita della paternità di opere originali [authoring]. Attraverso applicazioni di tipo diverso sarà possibile individuare la semantica di metadati più adatta agli scopi volta per volta perseguiti, ma una sintassi comune offrirà uno strumento uniforme per assicurare l'interfacciabilità ed effettuerà lo scambio di metadati fra applicazioni e server.

La definizione delle proprietà sarà in forma leggibile dall'utente e comprensibile per la macchina, e la sintassi di trasferimento si baserà sul linguaggio XML. La messa a punto della specifica RDF come infrastruttura per metadati e sintassi generale di rappresentazione della conoscenza ha fatto seguito alla definizione della piattaforma PICS (v. supra) (W3C 1998). La specifica RDF associata alla firma digitale offrirà la chiave per il commercio elettronico, la cooperazione ed altre applicazioni.

La specifica RDF costituisce al tempo stesso un modello di rappresentazione di metadati e una sintassi per l'espressione ed il trasporto di tali metadati. Il trasporto avverrà fra server e clienti eterogenei, e per l'RDF sarà prioritaria l'interfacciabilità. Come la PICS, essa non contiene glossari predefiniti per la creazione di metadati; chiunque potrà stabilire nuovi glossari. La diffusione di etichette di metadati conformi alla specifica RDF semplificherà le ricerche sul Web rendendole più precise, e anche gli agenti software automatizzati ne beneficeranno raccogliendo informazioni o eseguendo singole operazioni. Il meccanismo descritto è il frutto degli sforzi congiunti di più società, e costituisce un eccellente esempio di quanto viene comunemente definito uno standard aperto, operante entro quello che viene definito comunemente un "sistema aperto".

Una volta definita, l'etichetta Dsig dovrà essere diffusa nei confronti di ampie collezioni disponibili pubblicamente; tali collezioni possono assumere forme diverse: ai fini di questa presentazione verranno indicate in modo generico con il termine di soluzioni di immagazzinamento. Una soluzione di immagazzinamento deve possedere lo spazio sufficiente ad ospitare centinaia di milioni di record, e caratteristiche di trattamento tali da permettere la consultazione di indici o l'impiego di motori di ricerca.

Modalità di distribuzione delle informazioni digitali

Esistono due modalità fondamentali di distribuzione commerciale delle informazioni digitali: attraverso un supporto fisico oppure attraverso la rete. La distribuzione di informazioni analogiche ed anche digitali avviene da tempo attraverso supporti fisici. Ciò rappresenta in via primaria la conseguenza del concetto occidentale di proprietà intellettuale, basato sulla fissazione dell'opera: la fissazione privilegia la fisicità. Per l'utente finale è più facile relazionarsi ad un CD-ROM come ad una forma di proprietà intellettuale, proprio per gli attributi fisici che in esso si manifestano. Il supporto CD-ROM è finalizzato a riprodurre alcune delle caratteristiche dei beni economici standard, e ad eliminare alcune delle caratteristiche dei beni digitali: è difficile eseguirne una replica, e l'informazione in esso contenuta si identifica con gli attributi fisici del supporto.

Un modello possibile di distribuzione delle informazioni si basa sull'impiego di metadati e cifratura.

Un modello possibile di microtransazione si basa su tre componenti: il venditore (che può essere autore e proprietario dell'opera digitale), il cliente e la società di credito sotto forma di un centro di elaborazione pagamenti. Gli oggetti interessati dalla transazione sono: l'opera digitale, l'etichetta di metadati (Etichetta Dsig) e i fondi digitali. Il sistema richiederà la messa a punto di almeno due applicazioni: un'applicazione per la generazione di etichette, di cui si servirà l'autore unitamente all'applicazione che crea l'opera digitale, ed un generatore di firma da associare all'applicazione che gestisce la posta (ad esempio, un'applicazione plug-in del tipo PGP [Pretty Good Privacy] per il browser Web). Il sistema è progettato per gestire pagamenti di ridotta entità; pertanto, obiettivo prioritario è quello di limitare i costi aggiuntivi imposti dalla transazione. In un sistema del genere, la sicurezza può basarsi sul sistema della fiducia. Quest'ultimo può essere schematizzato come segue: chiunque sia un cliente di fiducia di un istituto di credito continua a godere di tale fiducia fin quando non viene meno ad essa.

È necessario introdurre elementi di sicurezza. Per identificare la firma del cliente e del venditore, la società di credito può ricorrere a sistemi di deposito della chiave [crittografica] oppure ad elenchi pubblici. Per identificare cliente e venditore, l'istituto di credito può fare riferimento alla propria base di dati relativa ai titolari di carte. Un ulteriore elemento di sicurezza può consistere nella limitazione del numero di transazioni giornaliere e mensili. Infine, la parte che conclude la transazione (ossia, l'istituto di credito) potrà inviare alle parti interessate conferma via e-mail.

Il deposito delle chiavi [crittografiche] (key escrow) è una prassi costosa e controversa. La sua attuazione su base globale appare quantomeno difficile, dato che essa viola prassi ormai consolidate di competenza dei singoli Stati. D'altra parte, elenchi pubblici uniti all'indicazione delle date di invio e scadenza delle chiavi pubbliche potrebbero costituire una soluzione economicamente praticabile ai fini di micropagamenti.

In un ambiente distribuito quale Internet, è necessario concepire la sicurezza in modo diverso rispetto alla sicurezza nel mondo fisico. La prima considerazione da fare è che tutto

è informazione, e la rilevanza dell'informazione (la sua esistenza) tende a zero in assenza di comunicazione. La necessità di garantire sicurezza su Internet non dovrebbe impedire di effettuare copie o di mettere in atto altri comportamenti illeciti.

Dovrebbe però impedire il re-indirizzamento di materiali generati in violazione di leggi o di un contratto fra le parti: perché è la reiterazione che può comportare un danno economico significativo per il venditore/l'autore, non già la copia occasionale. In un certo senso, questo approccio alla sicurezza può essere definito asincrono, rispetto alla sicurezza di tipo sincronico generalmente applicata alle transazioni.

Non c'è bisogno di creare un canale sicuro di comunicazione biunivoca fra venditore e cliente. Il cliente legge una dichiarazione certificata del venditore, e presume che l'identità del venditore e la sua dichiarazione siano degni di fede; l'istituto di credito legge la dichiarazione firmata dal venditore e dal cliente come transazione, e verifica l'identità del venditore e del cliente. Una volta che il venditore abbia ricevuto la sua etichetta di metadati, firmata dal cliente e dall'istitutodi credito, la transazione è completa. Anche in questo caso è possibile definire tale transazione come asincrona, rispetto alla transazione sincronica consentita dal protocollo SET (Secure Electronic Transaction - Transazione Elettronica Sicura).

III SESSIONE

Ing. Claudio Manganelli
Componente, Garante per la protezione dei dati personali

Abbiamo previsto un piccolo cambiamento del programma per mettere a fuoco il punto di vista del consumatore sul tema del commercio elettronico, e in particolare il punto di vista di un significativo rappresentante dei consumatori presso l'Unione Europea, il Commissario Emma Bonino. Pregherei la regia di far partire il filmato.

Domanda: Commissario Bonino, noi siamo in una settimana particolarmente importante per l'ingresso nell'Europa Monetaria. La legge sulla privacy ormai è in vigore da un anno; oltre l'Europa Internet è il villaggio globale, abbraccia il mondo. Come vede lei Internet e i problemi che inserirà in questo scenario.

Commissario Emma Bonino

Il più grande problema è che perdiamo il treno di Internet. È quello che mi preoccupa di più, ed è vero che l'Europa in quanto tale non è stata l'antesignana o all'avanguardia delle nuove tecnologie, è venuta al traino di iniziative e investimenti anche tecnologici che sono di matrice americana. Quindi l'Europa è arrivata già abbastanza in ritardo. All'interno della famiglia europea ci sono stati alcuni stati membri che sono più in ritardo di altri, l'Italia è certamente uno di questi. Quindi a me pare che il grande problema che io vedo di fronte è di non cogliere questa occasione, perché credo che la sfida sia tale che va al di là dei confini europei, come lei ha detto, che non basta un atteggiamento volontaristico di questo o di quel piccolo e medio imprenditore o di questo o quel personaggio individuale, ma se si vuole cogliere questa occasione, come io ritengo sia imprescindibile, bisogna richiamare anche investimenti e attenzione anche di responsabilità pubblica per tutto quanto riguarda la parte normativa, ma di liberalizzazione, quanto costa l'interconnessione nel nostro Paese, ma anche per quanto riguarda una serie di altri settori: l'alfabetizzazione informatica nelle scuole. Stiamo parlando di grandi priorità di bilancio e siccome il bilancio è quello che è, un grande dibattito culturale, di prospettiva di posti di lavoro, di tipo di società, che deve coinvolgere a mio avviso l'intero Paese.

Se vogliamo cogliere questo treno ed anche essere attori delle soluzioni, dei problemi che comunque questo treno comporta, questa è una grande priorità di bilancio, non è uno sforzo volontaristico di questo o di quel microsettore del nostro Paese.

Domanda: Lei ha richiamato l'attenzione sull'opportunità che i governi contribuiscano allo sviluppo di Internet, con facilitazioni fiscali piuttosto che pensare a tasse. Si ricorderà che i telefonini a suo tempo vennero tassati; oggi si parla già di tasse sui provider; secondo Lei, per poter diffondere il commercio elettronico piuttosto che il telelavoro, non sarebbe il caso che l'Italia seguisse l'esempio francese all'epoca di Minitel?

Commissario Bonino: comunque l'esempio dell'investimento o dell'incentivo pubblico.

Mi pare pazzesca l'idea di arrivare addirittura a tassare i provider. Noi prendiamo a parità di popolazione comparabile, sono collegati in Italia il 2% della popolazione, rispetto al Sud Africa il 3-3,5%, ma rispetto al 30% dei Paesi nordici o inglesi. Non parliamo degli americani. Eppure, nonostante questo, chiunque abbia letto il discorso dell'Unione del Presidente Clinton vede che ancora tutta la parte nuove tecnologie Internet e interconnessione ha la parte prioritaria dei prossimi investimenti degli Stati Uniti. Dico questo per dare la dimensione. In più, proprio in termini normativi c'è bisogno, a mio avviso di più liberalizzazione, di più mercato per esempio nella telefonia, bisogna assolutamente che non sia il

monopolista di ieri che si ricicla, ma alla fine ha lo stesso mercato, quindi padrone delle tariffe, semmai abbiamo bisogno di avere una molteplicità di provider e non un monopolio e credo che tutto questo implichi anche un atteggiamento normativo molto più liberale e non un atteggiamento normativo di ulteriore pressione fiscale o non fiscale o di ulteriore controllo.

Domanda: nell'ambito della Comunità, Lei ha particolarmente a cuore il problema dei consumatori, i consumatori avvicineranno il commercio elettronico se saranno certi che le loro transazioni verranno rispettate, la moneta verrà scambiata correttamente, non ci saranno fughe delle loro informazioni; vi sono anche dei problemi di privacy. Come vede questo scenario di fronte a due ipotesi: quella di studiare regole rigide e quella invece di definire poche regole ma sostenere l'autoregolamentazione dei provider.

Commissario Bonino: devo dirvi che sono molto più favorevole a questa seconda strada e anche chi è un grande sostenitore della prima non riesce mai a rispondere alla domanda: benissimo, ma se tu vuoi fare anche tante belle regole chi le applica e quali sono gli strumenti di controllo dell'applicazione? A questa seconda domanda, che non è proprio così marginale, perché il problema è se vogliamo fare regole o se vogliamo fare dei manifesti pubblici o degli appelli, questo è un altro discorso.

Io credo che uno dei punti fondamentali è che le regole, anche quelle del codice penale si applicano a Internet come a qualunque altro strumento e già ci sono. Il punto nodale è quello di capire sulla reperibilità e la responsabilità dell'autore. Io credo che il problema non sia mettere ulteriore limite a questa evoluzione, ma credo che una autoregolamentazione del provider sia una strada che, secondo me, ha più possibilità di dare più frutti.

Per quanto riguarda il consumatore compratore, dal punto di vista europeo siamo riusciti a far passare una direttiva almeno sulle garanzie delle vendite a distanza, che per ora si applicano solo ai prodotti, ma io mi auguro che ben presto riusciremo a fare anche la normativa sui servizi finanziari, perché un consumatore vuole essere più garantito se compra un'assicurazione piuttosto che se compra un paio di scarpe, se gli arrivano di un numero sbagliato, al massimo si arrabbia ma non è successo un dramma; se invece l'assicurazione non è più reperibile il venditore, al cosa diventa un pochino più preoccupante.

Esiste quindi una parte di normativa necessaria. Poche regole, ma poche regole applicabili e per il resto, io credo che bisogna puntare molto sulla concorrenza e sull'autoregolamentazione dei provider.

È vero che c'è un problema di privacy e di utilizzo dei dati. Forse questo è un tema su cui bisogna riflettere un attimo, ma senza pensare appunto che tutto si può risolvere con alcuni dati repressivi.

Grazie commissario, questa sarà una sfida per il prossimo anno, per noi ma anche per lei soprattutto. Buon lavoro.

Ing. Claudio Manganelli

Vorrei recuperare un iscritto a parlare della sezione precedente sul copyright, il dott. Jens Gaster, che sostituisce il dott. Reimbault ed è Amministratore principale presso la Commissione Europea dell'Unità che si occupa dei problemi del copyright e degli aspetti ad esso connessi. Grazie.

Mr. Jens Gaster

European Commission

Thank you very much, chairman, for the very kind introduction. Ladies and gentlemen, I am very honored to have the possibility to talk to you. My capacity is of European commission official who is heavily involved in the drafting and making of European copyright legislation. I think we have only the time to run through copyright in a nutshell. I must make some remarks concerning what we have achieved already, what is being proposed, and why. And I am also pleased to have the opportunity to respond to some of the criticisms of Professor Samuelson. Perhaps let me give first a few explanations of what is our role in all this. European commission and the other European institutions in their role as lawmakers do not invent the wheel. We have the task to approximate something that in many instances already exists.

All of our fifteen EU member states have copyright legislation. All of them are already bound by five EU Council of Ministers and European Parliament directives. Having said that, I may perhaps indicate why. Well, since the 1950's with the Treaty of Rome, the European communities are in existence. In the mid 1980's a single market was proposed, the internal market. And it is precisely because of this internal market mandate that the European Commission leads us to harmonizing copyright laws throughout Europe. We have to eliminate obstacles to trade in goods and services with copyrighted material and we have likewise to do away with distortions of competition.

In one huge economic space, it is not acceptable that exist different levels in the protection of copyright that are sometimes sky-scraping. So there were countries that protected almost everything let's say by copyright. And others copyrighted only works in which there was a very high level of creativity. And of course what was mentioned earlier today is enti-

rely true. Also within Europe initially, and I underline initially, we had two competing doctrine approaches. There are two common law countries and thirteen civil law countries. There are two copyright countries and twelve author-rights countries. And there is another country that is somewhere in between. So we did something there, and therefore since the end of the 1970's legislation setting out to harmonize such different approaches and harmonizing difficult issues, other issues of copyright law were considered. Since late in 1988 to a famous green paper already then called "Copyright and the Challenge of Technology," it was always the tip of the iceberg, a very comprehensive consultative exercise. So making European law requires years, if not decades, and all the time the public at large is consulted. In January '91, the working program was proposed of the decade to come.

This has since led to the adoption of the five directives to which I referred, two of which deal with digital technology. The first one is a computer-program directive dating from 1991 and the directive on the protection of databases was enacted in March of 1996. And that latter instrument is of crucial importance for the information society and the Internet. It applies already throughout Europe. The implementation deadline has passed and though the first objective this year is European law, it applies. I would like to point out, and this is one reply that I give to Professor Samuelson, that in many instances when you go on the Internet, you have to open a database. And therefore, the exclusive acts harmonized under the database directive apply in Europe.

They apply anywhere already. For example, copying, temporary storage, all this is already addressed in that directive. This is binding law in Europe. We have of course further to our hearings in 1994, the Green Paper dating from July of 1995, the Florence Conference in June 1996 and communication on the results of the second comprehensive consultation exercise in December 1996, now proposed another directive. It will be the seventh European copyright directive. I've skipped one. It is a 100% authors-rights measure. It deals with the authors' resale right. So you see, this is the authors' rights approach there. Well, this seventh one has been mentioned various times today. It is criticized largely. On the one-hand there are circles who consider that it goes by far too far; there would be over-protection. It is likewise the same amount of ink that's being used to criticize the other side of the spectrum. People claiming that it doesn't go far enough. We have to find a common denominator. The text is now before European Parliament for first reading and it will take some time until the final result comes out of the legislative process.

European Parliament and the Council of Ministers are co-legislators, and they do not act out of the blue. We will see what they will bring about with these very directives. What does it provide for, this proposal, and why? We must distinguish two very different things there. First of all, the proposal is designed to implement two international instruments that were adopted in December 1996 in Geneva. The WIPO Copyright Treaty and the WIPO Performers and Producers' Treaty, WPPT: Such two instruments also led, while they were in the making, to lots of controversies that have been settled since then. The treaties have been signed by all fifteen EU member states and the European Commission on behalf of the European Union. The European Commission has proposed just two weeks ago to ratify

such treaties. Therefore me must do our homework first.

We must implement the treaties and the EU member states which wish to do so separately, because new treaties are so-called mixed agreement, it means it must be done jointly, by the community and its member states because they share competence. The areas where the Union is exclusively competent, there are a few areas where it is to the member states, and then some other areas it is all mixed, so the entire text is a mixed agreement. This is 50% of the proposed directive, or even more, and of course the criticisms of technical devices largely concern the treaties that have already been adopted. We take to a large extent only text over from the treaties. But what is now special, additional, in the proposal? What is the WIPO plus? Well, it is a result of the consultation exercise.

Harmonizing throughout Europe the reproduction right included in exceptions, harmonizing the communication to the public right, including the famous making a bill right. This was proposed by Europe in Geneva and adopted at a world-wide level. It has set a significant issue of on demand delivery, the act of making available. This was needed because you have in Europe controversies about what is the public. You sit in your home and dial the disk or get a video on demand.

What is that ultimately? This issue has been addressed now. We have found a solution. Of course with the communication to the public right there must be also exceptions, but a few less than for reproduction. Now when it comes to the distribution in tangible form, you must of course harmonize a distribution right. Its most noteworthy exception being the exhaustion principle. A copy of the work in tangible form, a good has been re-sold with the consent of the right owner, because he will say 'I own that copy. This CD ROM is mine, and I want to do with it what I want to'. You are perfectly entitled to do so, when you acquire it lawfully. You can give it away to whomever you wish. No one can prevent you from doing so under the distribution right, it is exhausted, but only throughout Europe. Well, technical devices. I should not forget that.

They are of course dealt with also in this context. What has not been settled or what is about to be settled under this proposed directive and is in our initial working program, we have announced when we give some information about the results of the information society consultation exercise in December 96, that there would be a few other measures contemplated. We have not yet dealt with moral rights. They are of crucial importance, for example, for this country. I may refer to the famous Zimmerman case. We have neither dealt with collective rights management yet, or ethnic rights management systems. Some people feel we should deal with multi-channel broadcasting from a copyright perspective. A digital broadcasting right is demanded by some interests.

And last but not least, the issue of law enforcement, beyond what is now contemplated in the draft directive. All this will be dealt with later on. And one thing more. The issue of applicable law. Should there be a law prescribing the country of origin principle, as some major players believe, or should be there the traditional copyright concept, that where protection is sought, for that very tribunal here in Rome, for example.
Well, it's Italian copyright law that applies, and not the law of the country of transmission,

the country of origin. And by the way, in the Internet environment, where does that occur? We have heard today, well you know, we sent something over the Net, via different continents, you know, from Namur to Brussels. Where does the act occur? Whose Act applies? All are very difficult issues.
And I've of course omitted to mention another burning problem. Liability. The liability will be dealt with in a separate initiative commission services are currently preparing and I hope we will hear more about that tomorrow morning, I guess. Well, I could comment much more, but we have not the time for doing so. Let me before I end my intervention make two more remarks. When we talk about fair use exceptions, overprotection, freedom of information, abuses of monopolies and so on and so forth, you must clearly distinguish between protected works and non-works.
You must also take into account that Europe has different traditions, different to for example, the traditions of certain other countries who follow the common law approach or the copyright approach. So we have catalogues of exceptions in Europe, in continental Europe. We have traditional exceptions, and I make one remark in this perspective, because I think all EU member states, except the United Kingdom, provide for exceptions for works generated by the public authorities.
And of course copyright law is not alone in the world. There are all sorts of other regulations that might require the public authorities to make protected subject matter available to the citizens, in many cases for free. So therefore, I am not so much concerned about overprotection because we have not yet so defined of text here anyway.
We have to find a common denominator. And given that European legislation in the field of copyright is normally adopted with a huge majority or even by consensus - well, you can be sure we are trying our best to find the right balance. Thank you very much.

Jens Gaster

Intervento del Rappresentante della Commissione Europea

Grazie, signor presidente, per la sua presentazione. Signore e signori, sono profondamente onorato di avere la possibilità di parlare in questo consesso. Sono un funzionario della Commissione europea, e mi occupo in prima persona della redazione e della definizione di norme europee in materia di diritto d'autore. Credo che abbiamo solo il tempo di esaminare in estrema sintesi il tema del diritto d'autore.

Devo fare alcune osservazioni riguardanti i risultati già ottenuti, le proposte avanzate e i motivi. E sono particolarmente lieto di avere la possibilità di rispondere ad alcune delle osservazioni mosse dalla Prof.ssa Samuelson. Forse dovrei prima spiegare brevemente quello che è il nostro ruolo. La Commissione europea e le altre istituzioni europee in quanto operanti come legislatori non stanno inventando la ruota. Abbiamo il compito di ravvicinare qualcosa che, in molti casi, già esiste. Tutti i quindici Stati membri dell'UE hanno norme di legge in materia di diritto d'autore. Tutti sono già vincolati dalle cinque direttive del

Consiglio dei Ministri e del Parlamento europeo. Ciò detto, è forse il caso di indicarne le motivazioni. Bene, la Comunità europea esiste dagli anni '50, attraverso il Trattato di Roma. Verso la metà degli anni '80 venne formulata la proposta di un mercato unico, il mercato interno. Ed è proprio quest'ultimo mandato che spinge la Commissione europea a cercare di armonizzare le leggi sul diritto d'autore in tutti i paesi europei. Dobbiamo eliminare gli ostacoli allo scambio di beni e servizi relativamente ai materiali tutelati dal diritto d'autore, e dobbiamo al tempo stesso eliminare ogni forma di concorrenza distorta. In un solo grande spazio economico, non è ammissibile l'esistenza di livelli diversi di protezione del diritto d'autore - livelli che talora risultano elevatissimi.

In alcuni paesi esisteva una protezione praticamente totale, ad esempio attraverso le norme sul diritto d'autore; in altri si prendevano in considerazione solo quelle opere caratterizzate da un livello molto elevato di creatività. E ovviamente quello che è già stato detto in questa sede è del tutto vero. Anche in Europa avevamo inizialmente, e sottolineo inizialmente, due approcci dottrinari diversi: ci sono due paesi di *common law* e tredici paesi di diritto romano. Ci sono due paesi in cui si parla di copyright e dodici paesi in cui si parla di "diritti d'autore", mentre un altro paese si colloca su posizioni intermedie. Siamo quindi intervenuti in questo settore, e a partire dalla fine degli anni '70 sono state prese in considerazione disposizioni di legge finalizzate ad armonizzare i diversi approcci e a risolvere temi spinosi, oltre ad affrontare altri temi legati alla normativa sul diritto d'autore. A partire dalla fine del 1988 fino ad un celebre libro verde intitolato già allora "Il diritto d'autore e la sfida tecnologica", si è sempre trattato della punta dell'iceberg [di] un'attività di consultazione molto ampia.

Creare la legislazione europea è un processo che richiede anni, per non dire decenni, e tutto avviene sempre sulla base di una consultazione pubblica. Nel gennaio del 1991 è stato proposto il programma di lavoro del decennio successivo; su tale base si è giunti all'adozione delle cinque direttive di cui parlavo prima, due delle quali riguardano le tecnologie digitali. La prima è una direttiva sui programmi per elaboratori che risale al 1991; la direttiva sulla protezione delle banche dati è stata emanata nel marzo del 1996. Quest'ultimo strumento riveste un'importanza fondamentale per la società dell'informazione e Internet. È già applicabile in tutta Europa; il termine fissato per l'attuazione è già trascorso, e anche se quest'anno l'obiettivo primario è la legislazione europea, la direttiva è in vigore. Vorrei sottolineare, e in ciò rispondo ad una delle osservazioni mosse dalla Prof.ssa Samuelson, che in molti casi, quando si va su Internet, bisogna aprire una banca dati. E quindi, gli atti esclusivi armonizzati in base alla direttiva sulle banche dati trovano applicazione in Europa. Sono già applicabili dovunque. Per esempio, copie, registrazioni temporanee: tutto ciò è già regolato dalla direttiva; sono norme vincolanti in Europa. Poi, naturalmente, ci sono il Libro Verde pubblicato nel luglio del '95, a seguito delle audizioni tenute nel '94, la Conferenza di Firenze del giugno 1996 e la comunicazione sui risultati del secondo giro di consultazioni nel dicembre del '96: essi hanno condotto alla proposta di un'altra direttiva. Sarà la settima direttiva europea sul diritto d'autore. Ho saltato un punto. Si tratta di una misura fondata al 100% sui diritti degli autori, e riguarda il diritto di rivendita da parte dell'autore. Dunque, come vedete, in questo caso si è fatto ricorso all'approccio "diritti d'autore". Bene, questa settima direttiva è stata menzionata varie volte oggi, e molte sono le critiche avanzate. Da un lato ci sono quelli che ritengono che la direttiva si spinga troppo oltre, che si arri-

verebbe ad un'iperprotezione. Con la stessa veemenza e quantità di inchiostro vengono formulate anche le critiche opposte: c'è chi afferma che la direttiva non va abbastanza nella direzione giusta. Dobbiamo trovare un denominatore comune. Il testo è attualmente all'esame del Parlamento europeo, e ci vorrà del tempo per la conclusione del processo legislativo. Il Parlamento europeo e il Consiglio dei Ministri legiferano in comune, e la loro attività non nasce dal nulla. Vedremo cosa riusciranno a fare con queste direttive.

Ma che cosa prevede la proposta, e per quale motivo? Dobbiamo distinguere fra due aspetti molto diversi. In primo luogo, la proposta intende dare attuazione a due strumenti internazionali adottati a Ginevra nel dicembre del 1996: il Trattato OMPI sul diritto d'autore e il Trattato OMPI relativo a produttori ed esecutori. Anche questi due strumenti hanno suscitato, durante la loro definizione, numerosissime controversie che sono state successivamente risolte. I trattati sono stati firmati da tutti i quindici Stati membri dell'UE e dalla Commissione europea per conto dell'UE. Due settimane fa la Commissione europea ha proposto di ratificare tali trattati, e perciò ognuno di noi deve prima fare i compiti: dobbiamo dare attuazione ai trattati, e il fatto è che questo deve avvenire in modo congiunto trattandosi di accordi cosiddetti "misti": la Comunità e gli Stati membri condividono competenze. Ci sono settori per i quali l'Unione ha competenza esclusiva, e settori ove sono invece gli Stati membri ad avere competenza esclusiva, ed altri settori ancora in cui esiste una competenza mista - insomma, tutto il testo è un accordo misto. Ciò vale per il 50% della proposta di direttiva, e forse anche di più, e naturalmente le critiche di natura tecnica riguardano in gran parte i trattati che sono già stati adottati. In massima parte ci limitiamo a riprendere il testo dei trattati. Ma che cosa c'è di nuovo, di particolare nella proposta di direttiva? Qual è il differenziale OMPI? È il risultato dell'attività di consultazione. Armonizzare in tutta l'Europa il diritto di riproduzione anche per quanto riguarda le eccezioni, armonizzare il diritto di comunicazione al pubblico - compreso il famoso diritto di presentare una proposta di legge: questa è la proposta fatta a Ginevra e adottata a livello mondiale. Ha permesso di porre un quesito significativo in merito all'atto di fornire su richiesta, all'atto di mettere [qualcosa] a disposizione di terzi.

Era un'esigenza sentita, perché in Europa si discute proprio sul concetto di pubblico. Se a casa propria si ascolta un disco o si ordina un video, che cosa succede in ultima analisi? Questo problema è stato affrontato con il documento di cui parlavo. Abbiamo trovato una soluzione. Ovviamente anche per il diritto di comunicazione al pubblico devono essere previste alcune eccezioni, ma in misura minore che nel caso del diritto di riproduzione. Bene, quando si tratta di distribuzione in forma tangibile, occorre ovviamente armonizzare un diritto di distribuzione; l'eccezione più importante è rappresentata in questo contesto dal principio di esaurimento. Una copia dell'opera in forma tangibile, un bene viene rivenduto con il consenso del titolare, perché quest'ultimo afferma "Quella copia è mia. Questo CD-ROM è mio, e ne faccio quello che voglio".

È un diritto perfettamente legittimo, se lo si è acquisito legalmente. Si può cedere l'oggetto a chiunque si desideri; nessuno può impedirlo, in base al diritto di distribuzione, perché quest'ultimo è esaurito, ma soltanto in Europa.

Strumentazione tecnica: un altro punto da considerare. Anche in questo caso la proposta di direttiva affronta il problema. I punti ancora controversi o in via di risoluzione in base a

questa proposta di direttiva, contenuti nel nostro programma di lavoro iniziale, sono stati indicati nel dicembre '96, quando abbiamo riferito sui risultati dell'attività di consultazione relativa alla società dell'informazione annunciando che sarebbero state prese in esame altre misure. Non abbiamo ancora trattato del problema dei diritti morali. È un punto di importanza fondamentale; ad esempio, per quanto riguarda questo paese, potrei citare il famoso caso Zimmermann. Non abbiamo ancora affrontato il problema della gestione dei diritti collettivi, né i sistemi di gestione dei diritti [...]. Alcuni ritengono che dovremmo esaminare i sistemi di diffusione multicanale in un ottica di diritti d'autore; altri chiedono il riconoscimento di un diritto di diffusione digitale. E in ultimo, ma certo non meno importante, il problema dell'applicazione della legge, al di là di quanto attualmente previsto nella proposta di direttiva. Tutti questi aspetti verranno trattati in una fase successiva. E un'altra cosa ancora: il problema della legge applicabile. È preferibile una legge che prescriva il principio del paese di origine, come ritengono alcuni dei principali soggetti in gioco, oppure si deve applicare il principio tradizionale del diritto d'autore, quello fondato sul luogo dove viene intentata l'azione in giudizio - ad esempio il tribunale qui a Roma? Bene, si applica la legislazione italiana sul diritto d'autore, e non la legislazione del paese di trasmissione, il paese di origine. E, a questo proposito, per quanto riguarda l'ambiente Internet, qual è il luogo ove si verifica l'azione? Abbiamo sentito oggi l'esempio di un utente che invia un messaggio sulla rete, attraverso vari continenti - che so, da Namur a Bruxelles. Dove ha luogo l'atto? Quale legislazione si applica? Si tratta di temi molto difficili. E naturalmente non ho menzionato un altro problema di bruciante attualità: quello della responsabilità. Il tema della responsabilità sarà affrontato attraverso un'iniziativa distinta che stanno preparando i servizi della Commissione, e credo che se ne parlerà domani mattina.

Si potrebbero fare molte altre osservazioni, ma non ne abbiamo il tempo. Due ultimi rilievi, prima di concludere. Quando si parla di eccezioni riferite all'uso corretto, di iperprotezione, di libertà di informazione, abusi monopolistici, ecc., occorre distinguere chiaramente fra opere protette e non-opere. Bisogna inoltre considerare che in Europa esistono tradizioni diverse, ad esempio anche rispetto a quelle di altri paesi che seguono l'approccio di *common law* o basato sul diritto d'autore. È per questo che in Europa esistono veri e propri elenchi di eccezioni, almeno per quanto riguarda l'Europa continentale. Ci sono alcune eccezioni tradizionali, e da questo punto di vista vorrei fare un esempio specifico perché credo che tutti gli Stati membri dell'EU prevedano eccezioni per le opere prodotte da organismi pubblici - tranne il Regno Unito. E, inoltre, non esiste solo la legislazione in materia di diritto d'autore; ci sono tutta una serie di altre norme che magari comportano l'obbligo per gli organismi pubblici di mettere a disposizione dei cittadini opere protette - in molti casi a titolo gratuito.

Pertanto, non darei troppo peso al rischio di un'iperprotezione, dato che comunque non abbiamo ancora definito un testo del genere. Dobbiamo trovare un denominatore comune. E dato che la legislazione europea nel settore del diritto d'autore viene adottata in genere a larghissima maggioranza o addirittura all'unanimità - bene, potete star certi che stiamo facendo del nostro meglio per trovare il giusto equilibrio. Grazie.

REMARKS

Barbara Wellbery
Special Counsel for Electronic Commerce, United States Department of Commerce

Introduction

I am delighted to be here. And, I am honored to be here with the impressive array of expertise that the Data Authority has gathered from around the world. There is a tradition of dialogue between the United States and Europe on privacy issues going back more than 25 years. The United States is very indebted to the work Europe has done on the issue of privacy protection. I am pleased to be able to continue and add to that dialogue today.
I will speak today about electronic commerce and privacy - and the impact of each on the other. First, I would like to start by making explicit what the Clinton Administration means by electronic commerce and why we think it is so important. As Vice President Gore said last July:

"We are on the verge of a revolution that is just as profound as the change in the economy that came with the industrial revolution. Soon electronic networks will allow people to transcend the barriers of time and distance and take advantage of global markets and business - opportunities not even imaginable today, opening up a new world of economic possibility and progress."

Essentially, electronic commerce is the use of electronic networks - wired and wireless, satellite and terrestrial - for commercial transactions - from tracking inventory, to filling out loan applications, to market research, to actually buying and selling on line. I will use the term "Internet" throughout this discussion to refer to all electronic networks, whether they are open or proprietary and, therefore, not technically part of the Internet.

We expect the Internet and electronic commerce to transform classic business and economic paradigms. To provide just a few examples:

1. Electronic commerce will allow entrepreneurs to start new businesses more easily and with fewer up-front investment requirements by setting up web sites so that they can have access to the Internet's world wide network of customers.

2. The Internet will allow consumers to shop at home and to view products on their computers, even to visualize how they will fit together. It allows them to construct, for example, a room of furniture on their screens and to order and pay for their choices, all without leaving their homes.

3. The Internet can also change the nature of the relationship between retailers and their customers. One of electronic commerce's oft cited success stories is Amazon.com, the first Internet bookstore, which went from sales of less than $16 million in 1996, to sales of

$148 million in 1997. It offers its customers more than just books. It also offers on-line book clubs on subjects, authors, and books of interest to them, notifications of new books published by favorite authors and on specific subjects, and notifications about books by similar authors and on similar subjects. It offers its customers a virtual community, one not bound by physical location or real time.

We also expect electronic commerce to be the engine that drives our economy well into the 21st Century. The numbers we are beginning to see bear out this expectation. Last April the Department of Commerce released its first major study of electronic commerce entitled *The Emerging Digital Economy*. It describes the economic impact of electronic commerce.

The findings are quite impressive:

- Traffic on the Internet doubles every 100 days.
- In 1994, 3 million people used the Internet.
- In 1998, 100 million people are using it.
- By 2005, one billion people are expected to be users.
- We expect electronic commerce to surpass $300 billion a year by the year 2002.
- The digital economy is growing at 2 times the rate of the overall United States economy and now represents 8.2% of the United States GDP.
- In the last 3 years, information technology industries have been responsible for nearly 35% of total annual GDP growth in the United States.

But what does all this mean for privacy? A great deal, in fact. Much of the potential we see in the Internet and electronic commerce stems from the fact that they bring information to people on a global basis - and they permit both governments and the private sector to transmit, process, and store vast amounts of information about individuals easily and inexpensively. Increasingly, these capabilities are essential for governments to function effectively and for businesses to operate effectively.

In short, we are in the midst of an information explosion. We live in a world where information has become a commodity.

There is a darker side to this, however. In the course of using these networks, individuals create information trails that could provide others in the absence of safeguards with the personal details of their lives. Over the past several years, the United States and other nations have become increasingly concerned about finding ways in which privacy protection can be ensured. The challenge, in our view, is to balance the competing values of individuals' right to privacy with the free flow of information within nations and among them.

We think this is very important - not only because privacy is very important in its own right - but also because we don't think electronic commerce will develop to its full potential without privacy protection. But just as the Internet creates greater threats to privacy we anticipate that technology will offer many solutions to online privacy issues.

What are the implications for privacy policy? If information is the "capital" or the "money" of this new era, we believe we must be careful about how we interfere with its flow. In the United States, we have chosen a different approach to privacy protection than

that adopted here in the European Community. In part, we have done so because of our different legal and social traditions. But in a great part, we have done so because we believe the Internet and electronic commerce require a different approach.

The United States approach to privacy protection grows out of our tradition, which is deeply rooted in a concern about government excess. The First Amendment, a fundamental tenet of American democracy, requires that we balance the privacy rights of individuals with the benefits that stem from the free flow of information. In our experience, this balancing produces substantial personal, social, political, and economic benefits.

To achieve this balance, the United States has relied on a mix of sector-specific legislation, regulation, private sector codes of conduct, and market forces. When President Clinton issued "*A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE*" in July of last year, he emphasized the importance of addressing privacy concerns and a renewed commitment to self regulation.

The Administration also called for governments to recognize the Internet's unique qualities as they formulate policy. It's worthwhile to dwell for a minute on President Clinton's call for governments to recognize the unique qualities of the Internet. As I said earlier, the digital environment facilitates the collection, use, and instantaneous transmission of information that can diminish personal privacy. But in the context of the Internet with its global reach, traditional government regulation, constrained as it is by national boundaries, has limited utility. At the same time, the interactive capabilities of the Internet dramatically increase the likelihood that the market place will produce an optimal balance between data protection and freedom of information values. The rapid pace of technological development and the slow process of legislating also threaten to render legislation obsolete almost as soon as it is passed.

Given the Internet's unique qualities, the Clinton Administration believes that effective industry self regulation, coupled with sector specific legislation where needed, technology, and aggressive consumer education are the best way to protect personal information in the Information Age.

In addition, as we enter an era of expanded electronic commerce we need to keep in mind the following as we develop privacy policy:

- International flows of information are climbing rapidly within companies as they create global Intranets and between companies as they use Extranets. The continued growth in electronic commerce will also increase international data flows.
- The world has shifted from a relatively small number of mainframe computers to an enormous number of personal computers with the number of computer operators climbing correspondingly.
- Mainframe computer centers have security specialists and staff for complying with data protection rules. It will be hard to find the same expertise as the ability to process data is disseminated throughout a company. These changes mean that the costs and benefits of data protection rules have also shifted. We now have many more comp ters, inexpert personnel, and pervasive international transfers. The benefits of data

protection regulation are reduced because of the difficulties of enforcement.

Thus, in the United States we do not plan to adopt broad privacy legislation. Given what I have said earlier, that should not surprise you.

One of the basic tenets of our electronic commerce policy is that the private sector has to lead. But private sector leadership does not mean that the government simply gets out of the way and lets industry do as it wishes. Rather we are talking about a different kind of paradigm in which government and the private sector forge a new kind of partnership.

What this means is that we are working with the private sector to define the essential elements of effective privacy protection. We have developed a draft paper that identifies those elements. Those elements are based on the OECD Privacy Guidelines and include fair information practices. More specifically they include notice, choice, security, consumer access, and data accuracy as well private sector-implemented enforcement mechanisms.

Companies need to tell consumers what information they are collecting and how they intend to use it, and they need to give consumers the ability to limit use of their personal data. By enforcement we mean that consumers have to have a means of knowing that companies are actually doing what they say they are doing with consumer personal information, there have to be mechanisms for consumer recourse, and companies have to suffer some consequences if they do not do what they say they will do. We plan to ask the private sector for its views on our paper and work towards a consensus on these issues.

At the same time, and for the most part, we believe the private sector should take the lead in deciding how to implement these policies. Industry must take an active role in developing effective codes of conduct and in deciding how they will be implemented.

Exactly how verification will be done and what the mechanics of dispute resolution should be are in the first instance for the private sector to develop and implement. In our view, we believe government should intervene only if it appears that these mechanisms aren't working or that companies are not adopting these policies.

What is the private sector doing?

We understand that private sector consortia are being formed to develop effective self regulatory privacy codes of conduct. It is too early to know how extensive these efforts will be and whether these efforts will be successful. It is clear, however, that at this point consensus is emerging on such basic issues as the need for enforcement. Questions still exist on such issues as the extent of consumer access to information collected by companies and how exactly to provide enforcement. Fifteen trade associations in the high technology sector - representing over 20,000 companies - have come together to develop codes that contain the elements we have identified as essential.

We think in the long run a self regulatory approach to privacy will result in more effective and cost efficient privacy protection. Policies adopted by a company will apply anywhere the company does business. And, we will shift the burden and cost of enforce-

ment to the private sector. We also anticipate that technology will help solve privacy issues on-line. In our ideal world, consumers would have the tools to determine the level of privacy protection they wish to have - this could differ from consumer to consumer and, indeed, for any one consumer could differ depending on the particular circumstances of each transaction.

Such technology is in development, and is based on the technology developed to allow consumers to filter out content they do not wish themselves or their children to receive.

The technology, called the Platform for Internet Content Selection (or PICS), was developed by the World Wide Web consortium, an international consortium that includes universities located in the United States, France, and Japan.

This same consortium is developing P3P - a privacy vocabulary that could be used by web sites to evaluate the level of privacy they provide. Consumers would set their web browsers to visit only those sites that provide the level of privacy protection they wish.

The technology will also be designed to allow negotiations between consumers and web sites - so that companies could decide to offer a higher level of privacy in some circumstances and consumers could decide to accept less privacy protection in some circumstances. This technology is only a tool - it requires that companies or third parties rate web sites for privacy and that consumers set their browsers to accept only a certain level of privacy.

In sum, although we very much value privacy in the US, we have chosen a different approach to providing privacy protection than has been chosen here in Europe.

Indeed, when we view the Europe Union Directive on Data Protection we think it may inhibit the development of electronic commerce. The Directive tries to regulate closely something we think will be very hard to regulate in the information era. For example, the

Directive reads as if it were drafted for a mainframe world, where one could expect a relatively small number of hierarchical information processing systems. In the mainframe world, the concept of a data controller - one or several people in a company who determine the purposes and means of processing personal data - makes sense. But mainframes are the exception now and distributed decentralized networks are the rule. Who in a modern corporation with wide ranging distributed network processing would be the data controller?

According to the definition, it would be almost every corporate employee.

Nevertheless, or indeed, because of these problems, we are concerned about the impact of the Directive on flows of data between the United States and Europe. These are critical to commerce. As you know, the Directive would prohibit the transfer of personal information to countries that do not provide what the European Union considers to be an "adequate" level of data protection.

Under this provision, a multinational company could be prohibited from transferring any data from its European offices to the United States and other overseas locations. Thus, for example, a company might encounter obstacles sending personnel information back to the United States for payroll processing so that it pay its employees in Europe. The Directive will also affect the world of investment banking - and make it harder if not impossible for non-European Union firms to analyze European firms and to perform due

diligence and accounting audits on a consolidated basis for international companies.

We therefore think it is essential to find ways to ensure the continued flow of information after the Directive is fully implemented to avoid disruptions in trade. These could have disastrous consequences on both sides of the Atlantic. We would therefore urge you to strive for flexible implementation of the Directive here in Italy and to urge such flexibility to your colleagues in other member states and the European Commission. Such flexible implementation should ensure protection against real risks to personal privacy but as little interference as possible to the beneficial aspects of the free flow of information.

The United States is engaged in an informal dialogue with the European Commission at the subcabinet level on the Data Protection Directive. We will raise many of the points discussed above with the Commission as well as with many others.

I would like to close by emphasizing that inflexible implementation of the Directive places at risk not just trade with the United States, Japan, and many other countries. It also places at risk participation in the information economy and all the benefits it promises.

Barbara Wellbery

Consulente particolare per il Commercio elettronico

Introduzione

Sono felice di essere qui, oggi, e mi sento profondamente onorata di far parte di questo gruppo davvero notevole di esperti che il Garante italiano ha chiamato a raccolta da tutto il mondo. C'è una tradizione di dialogo fra Stati Uniti ed Europa sui temi legati alla privacy che dura da più di 25 anni. Gli Stati Uniti devono molto all'attività svolta dagli europei nel campo della protezione della privacy. Sono lieta di poter proseguire questo dialogo dando oggi il mio contributo.

Mi è stato chiesto di parlare di commercio elettronico e privacy, e in particolare dell'impatto reciproco. In primo luogo vorrei chiarire che cosa intende l'Amministrazione Clinton per commercio elettronico, e poi spiegare perché riteniamo che il commercio elettronico rivesta importanza primaria. Per citare quanto affermato dal Vicepresidente Gore nel luglio scorso:

"Siamo alla vigilia di una rivoluzione altrettanto radicale quanto il mutamento economico che ha accompagnato la Rivoluzione industriale. Ben presto le reti elettroniche permetteranno a tutti di superare le barriere di tempo e spazio e di beneficiare del mercato globale e di occasioni di commercio oggi inimmaginabili, aprendo un mondo del tutto nuovo di possibilità economiche e progresso."

Per commercio elettronico intendiamo sostanzialmente l'uso di reti elettroniche di qualunque tipo, cablate o meno, terrestri e satellitari, per condurre transazioni commerciali - dalle ricerche di inventario alla compilazione di richieste di prestito, alle ricerche di mercato, alla compravendita vera e propria on-line. Utilizzerò il termine Internet in riferimento a qualsiasi tipo di rete elettronica, aperta o proprietaria e quindi anche non facente parte tecnicamente di Internet.

Noi pensiamo che Internet e il commercio elettronico trasformeranno i paradigmi classici dell'economia e dell'impresa. Vorrei farvi solo qualche esempio.

1. Il commercio elettronico consentirà agli imprenditori di iniziare un'attività in modo molto più facile e con minori investimenti iniziali. Creando un sito Web, oggi le società possono avere accesso alla rete mondiale di clienti Internet.

2. Internet permetterà ai consumatori di fare acquisti a domicilio e di visionare i prodotti sul proprio computer, e addirittura di controllare gli accostamenti. Ad esempio, permetterà di costruire sullo schermo una stanza ammobiliata, ordinando e pagando i beni acquistati senza bisogno di uscire di casa.

3. Internet può anche modificare la natura dei rapporti fra rivenditori al dettaglio e clientela. Una delle storie più spesso citate a proposito dei successi del commercio elettronico riguarda una società statunitense chiamata Amazon.com. Si tratta della prima libreria Internet, che dai 16 milioni di dollari di fatturato nel 1996 è passata l'anno successivo ad un volume di affari di 148 milioni di dollari. Amazon.com offre alla clientela qualcosa di più della possibilità di acquistare libri: offre anche club del libro on-line su argomenti, autori e testi di interesse, segnala le ultime uscite degli autori preferiti e su argomenti specifici, e segnala anche libri di autori simili su argomenti simili. In sintesi, Amazon.com offre ai clienti una comunità virtuale, svincolata dai limiti spaziali o dal tempo reale.

Riteniamo inoltre che il commercio elettronico sarà il motore che guiderà la nostra economia verso il 21mo secolo. Le cifre che iniziamo a raccogliere confermano queste attese. Ad aprile, il Ministero del commercio ha pubblicato il primo ampio studio relativo al commercio elettronico, dal titolo "The Emerging Digital Economy" [L'economia digitale emergente]. In esso si descrive l'impatto economico del commercio elettronico.

I dati raccolti sono impressionanti:

- Il traffico su Internet raddoppia ogni 100 giorni.
- Nel 1994 gli utenti di Internet erano 3 milioni.
- Nel 1998 gli utenti sono 100 milioni.
- Entro il 2005 si arriverà probabilmente ad 1 miliardo di utenti Internet.
- Riteniamo che entro il 2002 il volume di affari del commercio elettronico supererà i 300 miliardi di dollari.
- Negli USA, il tasso di crescita dell'economia digitale è doppio rispetto a quello generale, e attualmente essa rappresenta l'8.2% del prodotto interno lordo.
- Negli ultimi tre anni il settore delle tecnologie dell'informazione ha generato quasi il 35% della crescita del prodotto interno lordo annuale statunitense.

Ma cosa significa tutto ciò in termini di privacy? Pensiamo che abbia una grande

importanza, perché buona parte delle potenzialità insite in Internet e nel commercio elettronico derivano dal fatto che essi rendono le informazioni disponibili per tutti a livello globale - e consentono ai governi ed ai privati di trasmettere, elaborare e memorizzare enormi quantità di informazioni sui singoli con grande facilità e a costi ridotti. Queste potenzialità divengono sempre più indispensabili ai governi per poter funzionare, ma anche alle imprese per operare in modo efficiente.

In sintesi, stiamo vivendo un'esplosione informazionale. Viviamo in un mondo in cui le informazioni sono divenute un bene di consumo.

Naturalmente tutto ciò ha anche un risvolto negativo. In effetti, utilizzando le reti elettroniche gli individui creano tracce informatiche che possono fornire a terzi, in assenza di tutele adeguate, informazioni personali sul loro stile di vita. Durante gli ultimi anni gli USA ed altri paesi hanno cercato in misura crescente di individuare strumenti per garantire la tutela della privacy. Nell'ottica statunitense si tratta di bilanciare i valori contrastanti del diritto delle persone alla privacy con la libera circolazione delle informazioni, a livello nazionale e internazionale. Riteniamo che si tratti di una sfida di grande importanza, non solo perché pensiamo che la privacy costituisca un valore importante di per sé, ma anche perché non crediamo che il commercio elettronico possa sviluppare tutte le proprie potenzialità senza un'adeguata tutela della privacy. Tuttavia, così come Internet pone minacce più gravi per la privacy, pensiamo che la tecnologia potrà offrire molte soluzioni ai problemi della privacy online.

Quali sono le implicazioni per quanto riguarda le politiche della privacy? Se le informazioni rappresentano il "capitale" o il "denaro" di questa nuova era, riteniamo che si debba usare molta prudenza nell'inteferire con il flusso di informazioni. Negli USA abbiamo scelto un approccio diverso da quello adottato qui nella Comunità europea. Si tratta di una scelta dovuta in parte alle diverse tradizioni sociali e giuridiche, ma in gran parte la motivazione va ricercata nella convinzione che Internet e il commercio elettronico necessitino di un approccio diverso.

L'approccio USA alla tutela della privacy nasce dalla nostra tradizione, le cui radici affondano nella preoccupazione per gli abusi di potere di parte governativa. Il Primo emendamento, che rappresenta un principio fondamentale della nostra democrazia, ci impone di bilanciare i diritti dei singoli alla privacy con i benefici derivanti dalla libera circolazione delle informazioni. Sulla base della nostra esperienza, questo bilanciamento genera grandi benefici personali, sociali, politici ed economici.

Per realizzarlo gli Stati Uniti hanno utilizzato una strategia multipla basata su legislazione settoriale, regolamentazione, codici deontologici settoriali e forze di mercato. Quando il Presidente Clinton rese pubblica, nello scorso luglio, la "Piattaforma per il commercio elettronico globale", sottolineò l'importanza di affrontare i problemi collegati alla privacy ed espresse il rinnovato impegno dell'Amministrazione nei confronti dell'autodisciplina.

L'Amministrazione inoltre invitava i governi a riconoscere le caratteristiche del tutto peculiari di Internet nella formulazione delle proprie politiche in materia. Vale la pena di soffermarsi un attimo sull'invito rivolto dal Presidente Clinton ai governi. Ho già detto che

l'ambiente digitale facilita la raccolta, l'utilizzazione e la trasmissione istantanea di informazioni che possono ledere la privacy degli individui; tuttavia, nel contesto di Internet, caratterizzato da una portata globale, le forme tradizionali di regolamentazione governativa hanno efficacia ridotta a causa dei vincoli imposti dai confini nazionali. Al contempo, l'interattività di Internet aumenta drasticamente la probabilità che il mercato realizzi un equilibrio ottimale fra protezione dei dati e libertà di informazione. Inoltre, la rapidità dello sviluppo tecnologico e la lentezza del processo legislativo rischiano di rendere immediatamente obsoleta qualsiasi norma di legge relativa ad Internet.

Tenuto conto delle peculiarità di Internet, l'Amministrazione Clinton ritiene che un'efficace autodisciplina settoriale unita, se necessario, a disposizioni di legge settoriali nonché all'uso della tecnologia e ad una campagna di educazione dei consumatori rappresenti l'approccio più indicato per tutelare i dati personali nell'era dell'informazione.

Inoltre, entrando nell'era del commercio elettronico diffuso, dobbiamo tenere presenti alcuni dati nella elaborazione di strategie per la privacy:

- I flussi internazionali di dati crescono rapidamente sia all'interno delle imprese, attraverso la creazione di intranet globali, sia fra le imprese, grazie all'utilizzo di extranets. La crescita costante del commercio elettronico non potrà che incrementare il flusso di dati a livello internazionale.

- Nel mondo si è passati da un numero relativamente contenuto di mainframe ad un numero enorme di personal computer, con un incremento conseguente nel numero degli operatori.

- I centri ove si trovano mainframe dispongono di specialisti in materia di sicurezza e di personale preposto all'applicazione delle norme relative alla protezione dei dati. Sarà difficile trovare lo stesso livello di competenza man mano che la possibilità di elaborare dati si diffonde ai vari livelli di un'impresa.

- Questi cambiamenti significano anche che si è verificato un mutamento dei costi e dei benefici inerenti alla normativa in materia di protezione dei dati. Oggi ci sono molti più computer, personale meno esperto e trasferimenti diffusi di dati a livello internazionale. I benefici derivanti dalle norme sulla protezione dei dati si riducono, essendo più difficile la loro attuazione.

Pertanto, gli Stati Uniti non pensano di adottare disposizioni normative di ampia portata; tenuto conto della parte precedente del mio intervento, questa affermazione non dovrebbe giungervi nuova.

Uno dei principi fondamentali della nostra politica relativa al commercio elettronico è quello di lasciare l'iniziativa ai privati. Ciò non significa, però, che il governo si tira da parte e lascia campo libero ai privati; stiamo parlando piuttosto di un modello diverso, in cui governo e privati stabiliscono un nuovo tipo di cooperazione.

Ciò significa che stiamo collaborando con il settore privato nella definizione delle componenti fondamentali per una protezione efficace della privacy. Abbiamo elaborato una proposta di documento in cui vengono individuati tali elementi. Si tratta di elementi basati sulle Linee-Guida OCSE in materia di privacy, e prevedono l'obbligo di un'informazione corretta. Più specificamente, essi contemplano l'informativa, la possibilità di scelta, la sicurezza, l'accesso dei consumatori e l'accuratezza dei dati, oltre a meccanismi di attuazione messi in opera dal settore privato.

Le società devono dire ai clienti quali dati raccolgono e come intendono utilizzarli, e

devono dare ai consumatori la possibilità di limitare l'utilizzo dei propri dati personali. Per attuazione intendiamo il fatto che i consumatori devono avere la possibilità di sapere che le imprese fanno effettivamente quello che dicono di fare con i loro dati personali; il consumatore deve avere la possibilità di fare ricorso, e le imprese devono subire conseguenze se non fanno dei dati personali l'uso che dicono di fare. È nostra intenzione sentire il parere del settore privato su questo documento, e collaborare nella ricerca di un consenso sui temi esaminati.

Al contempo, riteniamo innanzitutto che spetti al settore privato prendere l'iniziativa di decidere le modalità di attuazione di queste strategie. Il mondo delle imprese deve farsi parte attiva nella definizione di codici deontologici efficaci e delle rispettive modalità di attuazione. L'approccio adottato per compiere queste verifiche, ed i meccanismi di risoluzione delle controversie crediamo debbano essere definiti e messi in pratica dal settore privato. A nostro giudizio, l'intervento del governo è opportuno solo se risulta che questi meccanismi non funzionano, o che le imprese non adottano questo tipo di politiche.

Quali sono le iniziative del settore privato?

Sappiamo che sono in via di costituzione associazioni nel settore privato al fine di mettere a punto codici deontologici efficaci in materia di privacy. È ancora troppo presto per capire quale portata avranno questi sforzi, e se daranno risultati positivi; tuttavia, è chiaro che sta sviluppandosi un movimento di opinione favorevole rispetto a temi fondamentali come l'esigenza di dare attuazione a questi principi e di introdurre codici deontologici settoriali. Vi sono ancora dubbi, tuttavia, su temi quali il grado di accesso dei consumatori alle informazioni raccolte dalle imprese e le modalità specifiche di attuazione dei codici.

Quindici associazioni commerciali nel settore dell'alta tecnologia si sono coalizzate - e si tratta di associazioni che rappresentano oltre 20.000 imprese - per elaborare codici basati sugli elementi che abbiamo individuato come fondamentali.

Noi riteniamo che, nel lungo periodo, l'autodisciplina sia un approccio più efficace e proficuo in termini di costi/benefici per quanto concerne la tutela della privacy. Le politiche adottate da un'impresa troveranno applicazione in tutti i paesi del mondo in cui l'impresa opera, senza contare che i costi di implementazione vengono così a ricadere sui privati. Inoltre, ci aspettiamo che la tecnologia aiuti a risolvere on-line molti del problemi della privacy. Nel nostro mondo ideale, i consumatori avrebbero gli strumenti per definire il livello desiderato di tutela della privacy. Quest'ultimo potrebbe differire da un consumatore all'altro, e di fatto per ogni singolo consumatore potrebbe essere diverso in rapporto alle circostanze specifiche delle singole transazioni.

Questi strumenti tecnologici sono in via di messa a punto, e si basano sulle tecnologie elaborate per consentire ai consumatori di filtrare i contenuti che non desiderano ricevere o che non vogliono far giungere ai figli. Il World Wide Web Consortium, un consorzio internazionale che comprende università degli USA, della Francia e del Giappone, sta sviluppando questa tecnologia - detta PICS, ossia Piattaforma per la selezione dei contenuti su Internet (Platform for Internet Content Selection).

Lo stesso consorzio sta lavorando anche alla P3P - un glossario della privacy utilizzabile dai siti web per valutare il livello di privacy da essi offerto. I consumatori potrebbero set-

tare il proprio browser web in modo che visiti solo quei siti che offrono il livello di privacy da essi desiderato. La tecnologia dovrà in ultimo consentire la negoziazione fra clienti e siti web, così che le imprese possano decidere in determinate circostanze di offrire un livello più elevato di privacy, ed i consumatori di accettare, in determinate circostanze, un livello minore di tutela della privacy. Questo tipo di tecnologia è solo uno strumento: essa obbliga le imprese o i terzi a classificare i siti web in rapporto alla privacy, e impone ai consumatori di settare i propri browser in modo da accettare solo un determinato livello di privacy.

In sintesi, negli USA teniamo la privacy in grande conto, ma abbiamo scelto un approccio diverso alla tutela della privacy rispetto a quello individuato in Europa.
In effetti, analizzando la Direttiva dell'UE sulla protezione dei dati, riteniamo che possa inibire lo sviluppo del commercio elettronico. Pensiamo che miri a regolamentare rigidamente qualcosa che crediamo sarà molto difficile regolamentare nell'era dell'informazione.

Ad esempio, la direttiva sembra formulata in riferimento ad un mondo dove dominano i mainframe, caratterizzato da un numero relativamente contenuto di sistemi di elaborazione dati disposti gerarchicamente. In un mondo di mainframe il concetto di "titolare del trattamento" - una o più persone all'interno di un'azienda le quali decidono sulle finalità o le modalità del trattamento di dati personali - può avere un senso. Tuttavia, oggi i mainframe rappresentano l'eccezione, mentre le reti distribuite e decentralizzate sono la regola. Chi è il titolare del trattamento in un'impresa moderna, con tutta l'ampia gamma di trattamenti su reti distribuite che la caratterizza? Se si adotta la definizione contenuta nella Direttiva, titolare è in pratica ogni singolo dipendente dell'impresa.

Tuttavia, o meglio proprio alla luce di questi problemi, siamo particolarmente preoccupati per l'impatto della Direttiva sui flussi di dati fra Stati Uniti ed Europa. Questi flussi sono indispensabili per il commercio. Molti di voi sapranno che la Direttiva tende a vietare il trasferimento di dati personali verso paesi che non garantiscono quello che la Commissione europea ritiene essere un livello "adeguato" di protezione dei dati.
In base a tale disposizione, una società multinazionale si vedrebbe vietare il trasferimento di dati dalle sedi europee agli Stati Uniti e in ogni altra sede d'oltreoceano. Pertanto, sarebbe ad esempio difficile per una società inviare negli USA dati personali ai fini dell'elaborazione contabile per pagare i propri dipendenti in Europa. La Direttiva avrà effetti anche sul settore delle banche di investimento, rendendo più difficile, o addirittura impossibile, l'analisi di ditte europee da parte di ditte non appartenenti all'UE e la preparazione di revisioni contabili su base unificata per conto di società internazionali.

Pertanto, riteniamo che sia indispensabile trovare il modo di garantire che i flussi di informazioni proseguano anche dopo il pieno recepimento della Direttiva, evitando turbative nel settore del commercio. In caso contrario, le conseguenze sarebbero disastrose su entrambe le rive dell'Atlantico. Vi invitiamo quindi a puntare ad un'attuazione flessibile della direttiva qui in Italia, ed a sollecitare un'analoga flessibilità anche presso i vostri colleghi in altri Stati membri e presso la Commissione europea. Un'attuazione flessibile permetterà di garantire la protezione nei confronti di rischi reali per la privacy, interferendo il meno possibile con i benefici derivanti dalla libera circolazione delle informazioni.

Gli USA sono impegnati in una serie di colloqui informali con la Commissione Europea in merito alla Direttiva sulla protezione dati. Molti dei punti menzionati nel mio intervento verranno affrontati nel corso di tali colloqui con la Commissione e con molti

altri soggetti. Vorrei concludere sottolineando che un'attuazione inflessibile della Direttiva comporta un rischio non soltanto per le relazioni commerciali con gli USA, il Giappone e molti altri Stati, ma anche per la partecipazione all'economia dell'informazione ed a tutti i benefici che da essa sembrano poter derivare.

Ing. Claudio Manganelli

La dott.ssa Wellbery ci ha dato una visione completa del pensiero americano su questo tema, che sarà fonte di discussione sicuramente nei prossimi giorni.

Vorrei farvi sentire il parere di chi opera per il sistema bancario, il dott. Marco Bellinzoni, Vice Direttore generale della SSB, una società della quale si servono molte banche per gestire le transazioni legate ai movimenti fatti dalle carte bancomat e di credito, oltre che ad altri servizi bancari.

Dott. Marco Bellinzoni
Vice-Direttore Generale SSB

Siete mai stati sulle montagne russe?

In questo momento io ho questa impressione: mi sembra di essere al culmine, quando il vagone va molto lento e tutti i compagni di viaggio si chiedono insistentemente se il convoglio andrà, a che velocità andrà, se sarà sicuro e molte altre domande ancora.

Questa è l'impressione che ho avuto ascoltando gli interventi che mi hanno preceduto e le domande del pubblico.

Fermiamoci un momento e, prima di avventurarci in previsioni guardiamo a ciò che è successo nel recente passato.

In qualità di dirigente di una società interbancaria, la SSB, che presta da anni servizi a tutte le banche italiane, posso dire che il sistema bancario tratta una merce molto particolare, soprattutto quando svolge la sua funzione di fornitore di servizi di pagamento.

Le banche trattano solo informazioni, informazioni elettroniche scambiate fra di esse e con i loro clienti.

Per questa ragione il sistema bancario italiano e le società di servizi interbancarie come SSB hanno sviluppato un'esperienza di fatto nel trattare messaggi elettronici ad alto valore e ad alta criticità, in un certo senso anticipando in un ambito ristretto il concetto di *e-business*.

Vi illustro, con l'aiuto di poche immagini, alcuni esempi che riguardano la vita di tutti noi quando operiamo come clienti privati e quando operiamo all'interno di un'impresa.

Intendo qui riferirmi allo sviluppo delle transazioni di pagamento (puramente elettronico) effettuate con carta di debito *PagoBancomat* e allo sviluppo dei collegamenti diretti fra le imprese e l'intero sistema bancario - il "*Corporate Banking Interbancario*".

La possibilità di pagare con carta di debito Bancomat esiste in Italia dal 1985; ora osserviamo la curva che rappresenta il numero di operazioni effettuate dal 1989 al 1998.

Basta guardare i valori attuali di 140 milioni di autorizzazioni all'anno e la pendenza della curva che lascia intravedere il raddoppio delle operazioni nell'arco dei prossimi 18 mesi, per aver conferma che tutti i cittadini si sono abituati a utilizzare moneta elettronica e che pagare in forma elettronica è ormai un fatto familiare, più che prelevare banconote da un *Cash dispenser* per poi spenderle.

Parliamo ora di imprese: le imprese hanno la necessità di scambiare quotidianamente informazioni elettroniche con le banche: estratti conto, movimenti, saldi e di inviare disposizioni a valore contabile, quali bonifici, incassi, e altro. Le imprese italiane poi detengono conti correnti con numerose banche e pertanto necessitano di operare con esse in un unico collegamento e con un'unica modalità.

Da queste esigenze, dopo alcune esperienze di settore, alla fine del 1995 il sistema bancario italiano ha messo a disposizione il servizio di "*Corporate Banking Interbancario - CBI*"

Osserviamo il grafico e notiamo come in poco più di due anni siamo passati da zero a circa 300 milioni di operazioni all'anno, con un numero di imprese aderenti al servizio che sfiora le 90.000 e con circa 600 banche aderenti.

Questi due esempi: nel settore privato l'impiego di pagamenti elettronici con carta di debito e nel settore imprese il servizio CBI, ci raccontano del recente passato e ci insegnano che quando mettiamo a disposizione dei clienti soluzioni semplici ed efficaci nel rispondere alle loro esigenze, il successo è assicurato e la soddisfazione è reciproca.

Parliamo ora del presente, il commercio elettronico, della testimonianza delle banche italiane e di SSB.

Il commercio elettronico per le banche è prima di tutto servizi di pagamento sicuri ed affidabili su Internet; in questo campo SSB ha realizzato e avviato due servizi di pagamento:

Il primo, sviluppato da SSB stessa, si chiama *Telepay* ed è basato su sistemi di crittografia a chiave pubblica RSA con chiavi a 1024 bit cioè, detto in parole semplici, la protezione delle informazioni più forte che esista al mondo.

Il secondo, basato su standard internazionali sviluppati da VISA e MasterCard in collaborazione con i principali fornitori mondiali di tecnologie, si chiama SET e, ancorché basato sugli stessi sistemi di crittografia forte utilizzati da SSB in *Telepay*, prevede un iter di registrazione più complesso per i clienti e pertanto richiederà tempi più lunghi per la sua diffusione.

Per utilizzare *Telepay* un compratore deve soltanto avere una carta di credito, registrarsi da casa attraverso il suo computer sul sito di SSB e quindi effettuare, in tutta sicurezza i suoi acquisti su qualunque sito esponga il logo *Telepay*.

Numeri: in un anno e mezzo, dalla data di avvio del servizio ad oggi, abbiamo avuto l'adesione al servizio da parte di venti negozi e da parte di 40 banche che lo offrono.

Operatività: siamo stati mesi a contare le operazioni di acquisto fino a quando, ad un certo punto, abbiamo visto aumentare rapidamente il numero di operazioni. Si era attivato un nuovo negozio, una ricevitoria del lotto che accetta il pagamento delle giocate con *Telepay*; una vera ricevitoria del lotto che, oltre alla normale attività, ha realizzato un sito Internet nel quale, in collaborazione con una banca, accetta giocate e pagamenti con *Telepay*.

Questa esperienza insegna che i clienti sono pronti a rispondere attivamente a ciò che li interessa veramente e che li appassiona, o che è di grande utilità per loro, si tratti di acquistare computer o libri scontati del 40% o di altre idee interessanti. Ma abbiamo parlato molto di sicurezza, riservatezza e privacy. Tutti noi vorremmo poter fare delle operazioni su Internet, con delle controparti, siano esse banche, pubblica amministrazione, il mio medico, il vostro avvocato, decidendo se crittografarli e se firmarli in maniera elettronica. Questa possibilità oggi esiste, è una realtà.

La legge Bassanini, una delle più avanzate in Europa, stabilisce la validità legale delle firme digitali apposte ad operazioni o documenti; se la struttura legislativa è pronta, anche l'offerta tecnologica è pronta.

Oggi è disponibile per le banche italiane e per i loro clienti una architettura che consente di realizzare una sicurezza a tutto campo, dal cliente privato fino alla sua controparte finale per tutte le transazioni elettroniche, tipicamente per tutte le operazioni effettuate via Internet.

Ellips è il marchio che contraddistingue questa architettura all'avanguardia nel mondo che consente di rendere sicure, non falsificabili e non disconoscibili tutte le operazioni effettuate via Internet. Le applicazioni di questa nuova architettura vanno dalle operazioni effettuate con la propria banca, interrogazioni e disposizioni di qualunque tipo, al pagamento delle imposte, al completamento di atti notarili, al rapporto con la struttura sanitaria e molte altri ancora.

Tutto ciò che serve è dotarsi dell'architettura Ellips, che prevede l'utilizzo di un server Unix o NT presso il fornitore di servizi (la banca per esempio), l'impiego di software specifico sia sul server della banca che sul computer del cliente e, nei casi a più elevata necessità di protezione, l'impiego di una carta a microprocessore con algoritmo RSA residente.

Le chiavi segrete del cliente sono infatti memorizzate o in un dischetto opportunamente crittografato e protetto da una parola chiave o, appunto, in una carta a microprocessore, con RSA attivo, che oltre a memorizzare in forma altamente sicura la chiave segreta, effettua anche le vere operazioni di firma digitale. In tal modo nessun elemento di sicurezza esce mai dalla carta a microprocessore, che il cliente porta in tasca.

L'architettura *Ellips* ha ricevuto l'attenzione dei più avanzati produttori di tecnologia mondiale per il fatto di essere la prima (e per il momento l'unica) soluzione oggi presente sul mercato così completa e basata sugli standard di riferimento industriali PKCS11.

Abbiamo parlato di commercio elettronico e di sicurezza su Internet:

- pagare in maniera sicura → *Telepay e SET*
- crittografare e firmare qualunque operazione → *Ellips*

Vi ho portato l'esperienza in questi settori, vissuta dal punto di osservazione di SSB, una società che si trova al centro del sistema bancario; ora vorrei darvi due immagini di come è organizzato il sistema bancario e delle società interbancarie.

In questo esempio ho voluto rappresentare la banche, la Banca d'Italia, Monte Titoli e altre istituzioni, le imprese, i commercianti ed i privati che accedono ai servizi bancari attraverso le loro banche. I vari numeri di cui ho parlato prima si riferiscono a questo ambiente.

Questo è solo un esempio per dirvi come all'interno del sistema bancario ci siano delle strutture che spesso sono all'avanguardia in Europa per le loro singole attività e che, tutte insieme, forniscono alle banche i mezzi per essere competitive, per offrire a ciascuno di voi servizi vantaggiosi. Confezionare i servizi e proporli ai clienti di qualunque tipo è poi un compito che tocca alle banche.

Quali sono i miei suggerimenti, quali sono le mie aspettative, e che cosa penso potrebbe favorire la crescita del commercio elettronico in Italia?

Di tariffe telefoniche hanno già parlato i relatori che mi hanno preceduto e non aggiungerei altro al riguardo.

Potremmo però aggiungere che, come sono stati previsti incentivi di legge per la rottamazione delle auto, così potrebbe essere utile un analogo sistema di incentivi che favorisca lo sviluppo del traffico digitale (magari riducendo quello sulle strade reali, a beneficio di tutti noi); quindi incentivare l'acquisto di computer da parte dei privati e incentivare l'ac-

cesso a Internet. Assolutamente di primaria importanza poi, l'alfabetizzazione informatica: fare utilizzare regolarmente, e non come sporadiche attività di laboratorio, i computer dai ragazzi delle scuole per tutte le attività scolastiche.

Abbiamo citato prima l'esperienza del gioco del lotto su Internet: il commercio elettronico decolla quando trova applicazioni interessanti, appassionanti ed utili per i clienti.

Quindi, per esempio, perché non fare la spesa ad un supermercato via Internet chiedendo di consegnarcela a casa all'ora stabilita?

Se questo riguarda un esempio dei tanti, tratto dal settore dell'iniziativa privata, analogamente potremmo chiedere che la Pubblica Amministrazione ci consentisse di operare pienamente via Internet per tutte le richieste ed adempimenti nei suoi confronti: dalla scelta del medico di base e la prenotazione di visite ed esami presso le strutture sanitarie, al calcolo e pagamento di imposte e tributi a tutte le altre innumerevoli attività.

Solo dalla sinergia fra:

- incentivi all'adozione di computer da parte di privati
- iniziative di operatori privati di particolare utilità per i cittadini
- iniziative delle Pubbliche Amministrazioni locale e centrale

possiamo aspettarci che scaturisca il tanto promesso sviluppo dell'era digitale.

Ora possiamo ritornare sulla navicella che abbiamo lasciato all'inizio del discorso, riprendere il cammino e augurare buon viaggio a tutti coloro che parteciperanno a questo bellissimo e affascinante viaggio che è la scoperta del nuovo mondo digitale.

Ing. Claudio Manganelli

Ho vissuto gli inizi del bancomat, direttamente coinvolto nella vicenda; mi auguro che si avviino rapidamente anche le applicazioni finanziarie su Internet e il commercio elettronico. Sono necessari anche alcuni passi giuridici. La tecnologia è sicuramente pronta, ma servono regole, norme, e la contrattualistica; proprio sulla contrattualistica invito a parlare il dott. Alberto Gambino, avvocato e docente di diritto industriale all'Università Luiss, che è anche autore di un libro in tema di contrattazione a distanza, l'accordo telematico.

QUALI REGOLE PER IL COMMERCIO ELETTRONICO?

Alberto Maria Gambino

1. La riflessione del giurista su quali regole debbano presiedere al c.d. "commercio elettronico" risponde ad esigenze sempre più incipienti, dettate dall'enorme crescita numerica delle operazioni economiche effettuate in rete.

I dati parlano chiaro: secondo il rapporto della World Trade Organisation all'inizio del 2000 il numero dei navigatori in Internet salirà a 300 milioni dai 60 milioni attuali, e il commercio elettronico, valutato attualmente in 8 miliardi di dollari, supererà i 300 miliardi, una quota pari a circa il 2 per cento degli scambi complessivi dei paesi industrializzati. Inoltre, le aziende che operano nel settore realizzeranno, sempre entro il 2000, il 42 per cento del proprio fatturato grazie a vendite concluse in rete (questa quota è oggi del 15 per cento) e la sola pubblicità telematica produrrà un giro d'affari globale di 40 miliardi di dollari.

Anche le infrastrutture ed i servizi *online*, pari nel '96 allo 0,1 del Pil degli Stati Uniti, raggiungeranno i 100 miliardi di dollari (1% del Pil Usa).

2. Oggi le regole che dominano il commercio elettronico traggono la loro giuridicità più per un'adesione spontanea (o, forse, necessitata) degli utenti della rete, che non per una loro vincolatività normativa, che, per definizione, non ha una portata omogenea nello scenario dei rapporti giuridici attivati per mezzo della rete delle reti, qual è, appunto, Internet.

Sebbene infatti possano *aprioristicamente* ritenersi operanti anche in tale ambito i meccanismi dispositivi propri del diritto privato internazionale, volti a dirimere il conflitto tra norme peculiari a singoli ordinamenti - così sfatando l'illazione dell'esistenza di un singolarissimo "diritto cibernetico" - nondimeno occorre considerare che proprio la scelta dell'uniformità normativa ai soli fini dell'individuazione della legge applicabile induce ad una più larga riflessione sulla portata delle singole normative che *da più parti* incidono sulla materia.

Ma che modello di "uniformità" è più opportuno seguire?

È sufficiente la disciplina nazionale, pur integrata con i principi della prassi internazionale? Oppure l'iniziativa normativa deve partire dall'Unione Europea? O, infine, è più opportuna la predisposizione di una disciplina di origine convenzionale, cui aderiscano via via tutti i Paesi del mondo (predisposta da organismi come il WTO)?

Ciascun approccio possibile risponde ad opzioni di politica normativa che rivelano significative discrasie.

3. Un approccio che faccia leva sulla sola legge italiana, pur vivificata con l'ordinamento comunitario, si rivela sterile per due motivi.

Il primo motivo è di ordine applicativo: l'operazione ermeneutica svolta tradizionalmente dai giudici nostrani denuncia, nell'individuare il contenuto di leggi che hanno un

background sovranazionale, un procedimento di lettura con giudizio di valore assunto alla luce del solo ordinamento di riferimento territoriale, così disattendendo la natura stessa dell'affare commerciale elettronico, che è permeato da regole comportamentali di una prassi "telematica" a volte contraddittorie rispetto ai principi giuridici tradizionali (si pensi a quei boicottaggi - leciti in Internet - realizzati con reazioni *flaming* da parte di operatori danneggiati).

La seconda ragione di una inadeguatezza normativa legata alla sola legge nazionale si evidenzia nella scarsa possibilità di *enforcement* delle norme stesse. Le prime decisioni dei giudici italiani in tema di usurpazione di insegna commerciale e di marchio tramite *domain name* contraffatto sono significative: le corti di merito, pur meritevoli per lo spirito di adattamento al sistema del commercio elettronico, potranno difficilmente attuare i loro provvedimenti ove gli illeciti siano perpetrati attraverso *provider* che risiedono all'estero.

4. L'approccio comunitario si connota per una strategia che si può definire "centralistica": la regolamentazione del mercato digitale parte dalle istituzioni politiche a ciò preposte e implica soluzioni univoche a ciascun problema che il commercio telematico presenta.

Una tale "filosofia", nel tentativo di potenziare al massimo la certezza del diritto, non può però, nel contesto telematico, che disattendere la propria ragion d'essere.

Valga questo esempio: quando un acquirente francese compra *on line* un software americano venduto da un negozio presente nella rete attraverso un computer localizzato in Australia, chi pagherà l'Iva e a chi?

La globalità è dunque il parametro congenito al commercio elettronico, presupposto per la costruzione di un sistema.

Il cuore dell'approccio europeo può allora in quest'ottica fungere da criterio direzionale al metodo normativo prescelto: un'autorità centrale che disciplini globalmente il commercio elettronico. Ad esempio, con riferimento al settore della privacy, il metodo si tradurrà nell'istituire un'autorità regolatoria, cui notificare le operazioni di trattamento telematico dei dati personali al fine di un vaglio di legittimità.

5. Ma l'intervento regolativo, dunque necessario, può prendere sostanza da un terzo approccio alla soluzione del problema, coerente alla cultura nordamericana, incentrato sul principio di sussidiarietà: solo là dove gli operatori del mercato non sono in grado di autoregolamentarsi, interverrà un potere centrale.

In questo senso, le idee guida delle politiche nordamericane sul commercio elettronico si sintetizzano in cinque principi:

1) il settore privato guida lo sviluppo del commercio elettronico;

2) il governo si astiene dall'imporre limiti indebiti al commercio elettronico;

3) il governo interviene per sostenere e attuare un quadro giuridico di riferimento prevedibile, minimo, semplice e coerente per il commercio elettronico;

4) ciascun governo dovrebbe riconoscere le qualità uniche di Internet;

5) il commercio elettronico su Internet deve essere facilitato su base globale (qui potrà intervenire il WTO).

Per tornare all'esempio della *privacy*, secondo questo approccio, saranno gli stessi ope-

ratori di Internet a dotarsi di un codice di autoregolamentazione e contrassegnare i siti relativi a chi abbia aderito a tale codice con un "sigillo di qualità" visibile ai navigatori. Sarà poi il libero gioco del mercato a incentivare il rispetto di tali codici, presumendosi che il consumatore intratterrà rapporti commerciali preferibilmente con chi gli garantirà l'adeguata riservatezza dei dati immessi in rete.

Ma è chiaro che per una effettiva informazione dell'utente, oltre al marchietto di qualità, sulla pagina *web* dovrà essere indicato il *link* relativo al contenuto informativo del codice di regolamentazione adottato.

6. Con visione realistica, qualunque sia l'opzione preferita dagli organismi continentali, deve però constatarsi che con la filosofia e l'approccio nordamericano occorrerà comunque fare i conti e ciò per un semplice dato di fatto: gli Stati Uniti dominano l'intero scenario del commercio elettronico.

In quest'ottica sembrano riproporsi gli stessi presupposti che hanno visto l'implementare nel nostro ordinamento di principi sconosciuti come il diritto al *copyright* per la tutela del *software*. Non è casuale, del resto, quanto è accaduto con le normative sul *copyright* in relazione ai *database*, con la creazione di un nuovo diritto di autore *sui generis* e ciò su proposta della *World intellectual property organization*, poi scioltasi a Ginevra a fine 1996.

7. Ma alla nascita di una nuova "*economia Internet*" e al correlativo bisogno di aggiornamento delle norme su scala mondiale, anche la cultura giuridica del vecchio continente dovrà imporre i propri distinguo al fine di portare a compiutezza una l*ex mercatoria telematica* coerente alle aspettative dei consociati-utenti.

Le tematiche di forte interesse in tal senso si aprono a ventaglio numerose e collegate tra di loro: la tutela del contraente telematico, la sicurezza delle transazioni in rete, la firma digitale, la tutela del diritto d'autore.

I precipui caratteri della negoziazione telematica, ove primo fra tutti, incide la virtualità dell'acquisto, ovvero l'impossibilità di maneggiare e toccare i prodotti e di fare confronti di prezzo e valore tra marche diverse, come si può fare in un supermarket reale, impongono la necessità di una informazione del consumatore in grado di colmarne il *deficit* cognitivo.

La scarsa sicurezza della rete fa sì che pochi si fidano di spedire il loro numero di carta di credito, nel timore che venga intercettato e riusato abusivamente. In questo senso però c'è una convergenza di intenti tra l'operatore e l'utente, poiché il primo, proprio per il buon esito dei suoi affari, si industria continuamente a trovare modalità di pagamento sempre più sicure.

Con riferimento alla firma elettronica, il Regolamento attuativo della Bassanini, pur innovando, con il sistema delle chiavi asimmetriche, in termini di maggior certezza giuridica dell'affare concluso in rete e sicurezza dello stesso, rimane limitato al territorio italiano; e il presupposto per una sua estendibilità oltre i confini nazionali sarà quello dell'omogeneità del sistema di criptazione adottato da eventuali paesi stranieri.

Infine, il *modus communicandi* digitale e l'impatto sulle privative impone nuovi paradigmi di fruizione dell'opera creativa. L'atto dispositivo del bene immateriale per trasmissione non ha analogie con la cessione del *corpus mechanicum* distribuibile. Esiste un *right to*

read anzi un *right to browse*? Il computer è assimilabile al "brain" oppure la sua fixation non effimera nel cervellone implica una copiatura dell'opera e, dunque, dovrà imporsene la cancellazione oppure il pagamento di una *royalty*?

L'attuale mancata soluzione alle problematiche oggi sollevate dai temi enumerati si impone all'attenzione del giurista e dell'operatore, e spiega, allo stesso tempo, il perché l'acquisto in rete di generi di largo consumo, dall'abbigliamento agli elettrodomestici, sia ancora, soprattutto in Italia, insignificante.

8. Considerata la necessità di un approccio globale, si pone il problema di individuare un primo nucleo di diritti che dovranno sicuramente essere attribuiti a ciascun utente telematico. Tali diritti sono collegati a due principi cardine vigenti in ciascuna società che tragga dal diritto e dalla giustizia le proprie fondamenta, e dunque anche nella *cybersociety* della comunità Internet.

Il primo principio è di ordine sostanziale: ciascuno è responsabile dei propri comportamenti specie se questi violano i diritti di altri consociati.

Nella rete Internet è possibile incappare in operatori disonesti che, dietro l'apparenza di pagine *web* accattivanti, ove si offrono i prodotti più disparati, acquisibili dietro la digitazione del numero della carta di credito da parte dell'utente compratore, non mantengono affatto alcuna delle promesse fatte. La merce non presenta le qualità promesse e talvolta addirittura non viene neanche inviata; l'invio del proprio numero della carta di credito offre all'operatore senza scrupoli la concreta possibilità di svuotare il conto in banca dell'ignaro e forse un po' sprovveduto consumatore. A fronte di tutto ciò il consumatore non saprà con chi prendersela ove l'operatore telematico si presenti dietro le spoglie di un nome fittizio oppure non abbia alcuna stabile organizzazione che ne permetta l'individuazione fisica.

L'unico rimedio ipotizzabile è allora quello di una significativa maggior responsabilizzazione del provider, che permette a tali operatori commerciali la connessione in rete.

In quest'ottica, già nel settore dei mezzi di comunicazione di massa la giurisprudenza ha stabilito che il proprietario di un canale di comunicazione destinato al pubblico ha precisi obblighi di vigilanza sul compimento di atti illeciti, concorrenza sleale e illegittima appropriazione delle privative da parte di coloro che utilizzano il mezzo di comunicazione.

A tal fine, la rete Internet è stata equiparata ad un organo di stampa, con conseguente dichiarazione di responsabilità di un *provider*, che aveva permesso la diffusione per via telematica di segni distintivi contraffatti.

9. Tale principio di diritto sostanziale sarà peraltro puntualmente disatteso ove non si tenga presente il secondo principio cardine delle comunità democraticamente organizzate: l'effettiva attuazione (*enforcement*) del diritto.

Il *punctum dolens* per una reale diffusione di un'atmosfera di lealtà e correttezza che leghi gli operatori telematici ai consumatori si sintetizza proprio nella consapevolezza da parte di questi ultimi delle scarse possibilità di una tutela effettiva ove siano lesi nelle loro prerogative consumeristiche. Magistrati virtuali, mediazioni e arbitrati per via elettronica sono state le risposte che la comunità Internet ha tentato di offrire: ma la partecipazione solo volontaria a tali lodi ha inficiato la garanzia che il consumatore non sia in balia del libero arbitrio dell'operatore che discrezionalmente deciderà se partecipare o meno alla risoluzione telematica delle controversie.

D'altro canto l'imbarazzo dei giudizi nazionali è stato eclatante ove abbiano tentato di "oscurare" server localizzati in Paesi stranieri, e anche qualora vi siano riusciti, l'imbarazzo è addirittura aumentato alla verifica che il messaggio o la proposta contrattuale censurati conti-

nuavano a circolare nella rete Internet, che per definizione è acefala.

10. Una realistica soluzione ai problemi enunciati che tenga in debito conto sia la regola sostanziale di una tutela del consumatore telematico, sia il principio dell'effettività di tale tutela, appare allora quella di responsabilizzare i *provider* attraverso una vigilanza obbligatoria sui propri operatori inserzionisti.

I *provider* dovranno verificare tramite i tradizionali certificati commerciali che gli operatori inserzionisti abbiano i requisiti per svolgere in modo efficace ed onesto l'attività commerciale; pubblicizzare l'entità fisica (la stabile organizzazione) che sta dietro ciascun operatore telematico; imporre dei codici di autoregolamentazione a ciascun inserzionista. A tali fini è chiaro che occorre una convenzione su scala globale che sancisca i principi appena enunciati.

Ma proprio la difficoltà di una rapida soluzione della problematica in sede di organismi transnazionali, considerato soprattutto le diverse culture più o meno spiccatamente liberistiche rappresentate in tali consessi (si ricordi l'egemonia nel settore degli U.S.A.), può, allora, in seconda battuta, suggerire un secondo approccio.

A fronte del più restrittivo onere di vigilanza obbligatoria dei *provider* sui propri inserzionisti si potrebbe ripiegare su un onere di trasparenza, che significa obbligo di tenere al corrente i consumatori sull'an e il quomodo di norme comportamentali vigenti nelle operazioni commerciali attivate in rete, le quali offrano, per gli eventuali conflitti, meccanismi arbitrali alternativi alla giurisdizione ordinaria. In questa ipotesi ciascun provider potrà non aderire a codici di comportamento che dettino regole da far rispettare ai propri inserzionisti; tuttavia tale mancata adesione dovrà essere palese. Ciascun utente telematico potrà dunque scegliere, visionando un sigillo o un'icona telematica, apposta sulla pagine web, se contrattare con quell'operatore anche ove sia debitamente specificato che quest'ultimo non ha aderito e non intende aderire ad alcun codice di comportamento.

Tale consumatore telematico ove frodato, quantomeno, dunque, sarà stato preventivamente avvertito delle conseguenze di una difficile tutela per mancanza di un codice di autoregolamentazione specifico, lasciata infatti alle sole autorità giudiziarie ordinarie che, come si è detto, non sono in grado di garantire l'effettiva attuazione dei loro provvedimenti.

11. Vi è infine un'altra prospettiva di protezione, la quale mantenga intatti i meccanismi di sussidiarietà propri della cultura egemone nella rete, ma allo stesso tempo garantisca dalle "patacche" telematiche in cui, navigando, potrebbero incappare gli utenti.

Tale ipotesi di lavoro consiste nell'obbligatorietà di un'assicurazione assunta dagli operatori del commercio elettronico. *De iure* condendo ciò potrebbe "economizzare" i contenziosi attivati dagli utenti e garantire una maggiore fluidità al mercato in rete; e, al contempo, permettere che anche il solitario navigatore telematico si liberi, lasciandolo agli antichi, del memore richiamo: "*naufragium feci, bene navigavi*".

Ing. Claudio Manganelli

Si conclude la giornata, vorrei dire a quanti sono interessati a seguirci anche domani nelle due sezioni, altrettanto importanti sui diritti e responsabilità, autodisciplina e sugli approcci USA ed europeo a confronto, che cominceremo alle ore 9. Grazie.

II GIORNATA - SABATO 9 MAGGIO 1998
IV SESSIONE

Cons. Giovanni Butarelli

Buongiorno a tutti e grazie per essere tornati per questa seconda giornata del Convegno su "Internet e Privacy" che si preannuncia assai intensa. Abbiamo un calendario molto stretto di interventi, che vedranno, nella seconda parte della mattinata, nel corso della sessione presieduta dal prof. De Siervo, l'intervento in videoconferenza del Commissario Europeo Monti e un intervento del Ministro italiano di grazia e giustizia che ha seguito da vicino l'approvazione delle leggi sulla tutela della riservatezza.

In questa prima sessione sui diritti e le responsabilità, cercheremo con l'aiuto di un apprezzatissimo relatore e anche di alcuni interventi di fare il punto della situazione sul dibattito che riguarda le diverse posizioni di utenti e di fornitori di servizi e di accesso. Un dibattito che è assai recente, forse risale a sette-otto anni al massimo, ma che oggi, guardando le teorizzazioni di qualche tempo fa sembra lontano anni luce.

Il rapido evolvere di tecnologie ha reso infatti obsolescenti non soltanto i mezzi, le infrastrutture e gli strumenti ma le stesse costruzioni concettuali che si sono avvicendate.

Gli stessi diritti e le responsabilità si sono evoluti e hanno cambiato di contenuto con una velocità tale da porre in crisi non solo chi fa le leggi, ma anche chi le commenta, chi le applica e chi le dovrebbe conoscere.

Probabilmente il dibattito mondiale su Internet e la privacy è giunto ad un punto di maturazione che forse permette di trarre una sintesi, di intraprendere alcune misure che possono reggere il confronto anche con questa o con quella nuova applicazione che dovesse risultare in voga in Internet nelle prossime settimane.

Così come si sono rivelate infondate le preoccupazioni di chi lo scorso anno paventava la chiusura di Internet in Italia, addebitandone la morte alla legge sulla privacy entrata in vigore un anno fa, credo che siano da dissipare già oggi le preoccupazioni di chi ritiene che la piena applicazione, nell'ottobre di quest'anno delle direttive europee, possa comportare un blocco nei flussi di dati in Internet da e verso l'Europa.

Dico questo non per diplomazia istituzionale, ma perché ritengo che le direttive europee e le norme che le stanno attuando siano più flessibili di quanto si pensi e offrano una varietà di strumenti operativi sia agli utenti che ai provider, a cominciare dai modelli inter-

nazionali di contratto per finire con i codici deontologici di respiro europeo.

Certamente questi strumenti occorre sfruttarli; occorre cogliere le opportunità che le regole sulla privacy offrono, regole che obiettivamente sono complesse, non possiamo nascondercelo, ma che non devono essere oggetto di un rifiuto pregiudiziale solo perché non sono semplici da digerire o perché presuppongono un certo impegno nella lettura e, se posso dire, anche un minimo di fantasia nella loro applicazione.

Parlavamo del dibattito su Internet ormai lontano. Sappiamo tutti che ci sono stati due grossi orientamenti che si sono confrontati: un primo orientamento volto ad una iper-regolamentazione, molto eccessiva e anacronistica, non soltanto perché destinata a fallire in relazione alle nuove tecnologie, ma anche perché basata su eccessive cautele, forse anche per finalità pubbliche di indagini. Un'altra tendenza, invece, alimentata soprattutto da istanze giustamente libertarie, che rifiutava qualunque regolamentazione.

Una seconda tendenza, anch'essa destinata a non avere un seguito, non soltanto per le difficoltà di dare una tutela agli utenti più deboli e ai provider, ma anche perché in realtà rispetto ai flussi di dati una regola da applicare comunque c'è, negli studi giuridici si insegna sempre che un caso finisce sempre per essere regolato in un modo o nell'altro e forse, a rimetterci possono esserci appunto le categorie più deboli.

Si parla oggi di una terza via, ma che cosa è questo? Uno slogan come i tanti che si sono avvicendati negli anni scorsi? Ricordate tutti che si parlava di autostrade dell'informazione e qualcuno teorizzava un codice della strada molto dettagliato.

Si è parlato poi di una libertà assoluta. Che cosa è oggi questa terza via? E' una soluzione che veramente permette di miscelare una base di fondo di regole giuridiche con tutta una serie di strumenti flessibili, che possono riguardare l'aspetto contrattuale, che possono riguardare l'aspetto deontologico, che possono riguardare la ricerca, gli incentivi verso la creazione di tecnologie cosiddette pulite.

Sono queste le domande che oggi poniamo ai nostri relatori e interventori di questa sessione: quali diritti e quali responsabilità per gli attori della rete? E soprattutto come garantirli? Non è l'ora e l'occasione per trarre delle conclusioni e non intendo mortificare il dibattito, però credo che sia opportuno dire che sbaglia chi pensa che le leggi tradizionali sulla privacy possono essere applicate automaticamente, senza bisogno di qualche adattamento. E questo è facile constatarlo anche guardando le leggi italiane che contengono, come sapete, una disposizione abbastanza originale che prende atto di questa difficoltà di un'applicazione automatica di queste disposizioni e richiede degli adattamenti, ma degli adattamenti a quale scopo? Quale deve essere l'obiettivo di questa precisazione normativa?

Fino a che punto poi può spingersi il legislatore?

Uno dei tanti slogan che si sono avvicendati in passato si è basato su questo assunto: ciò che avviene online non deve essere guardato con sfavore rispetto a ciò che avviene off-line.

Ebbene, ci chiediamo, questo assunto può essere rovesciato nel senso che si può affermare che anche online occorre garantire ciò che avviene off-line, e occorre garantirlo con nuove regole o è sufficiente adattare quelle che già esistono nell'ordinamento?

Qualcuno, leggendo la legge italiana sulla privacy, ma il discorso potrebbe valere per le

altre norme, ha ipotizzato una grande difficoltà per i provider di applicare le normative che riguardano il flusso dei dati verso l'estero e ha quindi ipotizzato una grande difficoltà. Ma ci chiediamo: siamo proprio sicuri che gli strumenti che, certo, devono essere specificati, sviluppati, interpretati, applicati, non offrono già una base generale di intervento attraverso delle garanzie efficaci e non di puro stile date da formule contrattuali, attraverso dei codici deontologici. C'è bisogno veramente di garantire che la posta elettronica sia uno spazio garantito anche dalla nostra Costituzione, o possiamo arrivare a questo in base alla stessa interpretazione della norma costituzionale, prima ancora di guardare alle norme che hanno interpolato il codice penale.

Negli ultimi giorni qualcuno ha sollevato difficoltà applicative della legge sulla privacy lamentando che i provider non informano gli utenti rispetto ai cosiddetti trattamenti invisibili.

Ebbene, ci chiediamo, quanti provider hanno attuato realmente la legge che riguarda l'obbligo di informativa degli utenti e spiegano con parole semplici agli utenti quali sono i loro diritti? C'è proprio bisogno di cinque pagine per spiegare che c'è un certo trattamento che riguarda l'utente o alcune formule, in stile comunicativo molto semplice, possono raggiungere l'effetto, lo spirito della norma? Non vogliamo fare apologia delle nostre formule, ma nel modello di adesione al convegno avete trovato un'informativa di cinque righe che spiega che uso viene fatto dei dati raccolti in occasione di questo convegno, e ci chiediamo se altrettanto non possa avvenire per quanto riguarda i trattamenti che avvengono in rete.

Se ci colleghiamo con il sito web della Commissione Garante francese, notiamo che, a scopo educativo, c'è una adeguata informativa rispetto al trattamento dei dati che riguardano chi si connette con il sito stesso.

Anche per quanto riguarda la conservazione da parte dei provider dei cosiddetti log, cioè dei dati che riguardano le operazioni, c'è proprio bisogno di nuove norme o è sufficiente applicare quelle già esistenti?

Ai nostri relatori chiediamo anche di vedere come i diritti si possono armonizzare.

Opportunamente, questo convegno è stato orientato anche verso la proprietà intellettuale, il commercio elettronico, e non a caso; se guardiamo ad esempio le direttive europee che ieri sono state ricordate, possiamo notare come in queste direttive, che nel nostro Paese devono essere attuate, si ipotizza anche un diritto nuovo, un diritto che non a caso è stato definito *sui generis*, quello di impedire l'estrazione sleale di determinate informazioni che non hanno un volume tale da essere protette sotto il diritto d'autore, perché non sono di complessità tale da avere carattere di originalità, ma pur sempre possono essere utilizzate solo con certi comportamenti, con certe prescrizioni.

Come conciliare questo diritto a una tutela *sui generis*, che viene dal mondo della proprietà intellettuale, con il principio della libera circolazione delle informazioni, che invece è affermato nelle direttive europee sulla protezione dei dati?

Qualcuno potrebbe dire che nell'una direttiva e nell'altra c'è una clausola di salvaguardia dell'altra disciplina, e questo è vero, ma poi, quando andremo ad applicarle in concreto, come avremo la possibilità di conciliare questi diritti?

L'ultima domanda che si pone per i nostri relatori e interventori è se i diritti e le responsabilità che si prefigurano in rete siano delle nuove posizioni soggettive o possano, almeno in parte, essere considerate delle forme di manifestazione di diritti che sono già riconosciuti costituzionalmente in ciascuno dei nostri Paesi.

Non voglio anticipare certamente conclusioni, ma forse c'è la possibilità di tener conto che alcune nuove posizioni soggettive si vengono configurando. Il diritto di informativa è certamente già affermato dalle leggi sulla privacy, ma che dire del diritto del navigatore, dell'utente di essere consapevole degli effetti reali delle sue navigazioni in rete. Non è tanto un diritto di conoscere puramente e semplicemente i trattamenti di dati che lo riguardano, ma il diritto di conoscere gli effetti dei suoi comportamenti. E questo diritto come va attuato?

Attraverso delle *guidelines* come quelle che il Consiglio d'Europa si appresta a varare, o come quelle che l'Autorità garante spagnola ha approvato in forma di raccomandazione agli utenti e ai fornitori? Oppure c'è bisogno di qualche cosa d'altro?

Ho posto forse troppe domande, e me ne scuso, ma era in apertura di mattinata un intervento volutamente stimolante.

E' con vivo piacere che do la parola al prof. Herbert Burkert, senior research fellow presso Saint Augustin in Germania, il quale oltre ad essere un apprezzato esperto della materia, è una persona che ha avuto importanti incarichi presso il Legal Advisory Board, la struttura che presso la DGXIII della Commissione europea segue queste materie con un approccio uniforme. Prego professore.

RIGHTS AND RESPONSIBILITIES

Herbert Burkert

1.Introduction

Change and the law

We are living in old societies with new technologies. How are we to find out when, and where, and how these technologies should change the web of old rights and responsibilities we are living in? Change will certainly occur, but should we enforce it with the help of our legal system? This fundamental question on the role of law in our Informational Society (I am using Manuel Castell's term here) has many answers. One of the answers is that new technologies always also incorporate dreams on how societies should be, if only they could be, while our current laws is always the frozen political compromise of a given time.

The essentially new

New technologies tend to defreeze such compromises and legitimate the discussion on change. What sort of change is strongly connected as to what is perceived as the essentially new that seems to be arriving with the new technology. This essence - in my view - is the creation of a "total communication environment".

Total communication environment

In this environment it is technically possible that every individual communicates with every other individual by using whatever medium - sound, vision, even touch - regardless of barriers of time, space, complexity and culture. I call this environment "total" communication environment because all these communications - with the same ease - can themselves become objects of communication - for whatever purposes.

Power question

This essence poses an essential problem: The technology is enhancing power exponentially, and therefore what I only have described as a *possibility* for individuals is a *certainty* for organizations. In the interest of social cohesion, where there are more and less organizable interests, this gap needs to be bridged, and this is where new rights and new responsibilities - which will turn out to be not that new after all - will have their role to play.

2. Rights

Two basic groups

I see two basic groups of rights evolve, leaving their footprints already in our current legal systems:

- rights to communicational inclusion, and
- rights to communicational exclusion.

2.1 Rights to Communicational Inclusion

These rights first of all comprise:

2.1.1 The right of access to the means of communication

Concept

This right has many facets. In order to participate in the pursuit of happiness, to enjoy one's liberties and to participate in the fate of one's community in a total communication environment one must have access to the *means* of communication and to the knowledge of how to use them. The right of access to the means of communication in an affordable way is therefore one of the basic elements of rights to communicational inclusion.

Traces

We find first traces of this evolving right in the concept of universal service within the framework of telecommunications regulations.

2.1.2 The right to a communicational personality

Concept

In the total communication environment we will communicate as medial replicas of ourselves. To possess and to command such replicas will become an essential necessity to participate in commercial exchanges, to communicate with civil authorities, to exercise our civic rights, and even to stay in contact with our families and friends. The electronic signature and the email-address are examples of such replica through which we exist in the total communication environment. The more encompassing this environment will be the more essential such electronic replicas will become: They will become an essential expression of being a person with a legal status. Just as this status cannot be removed in total from a person, so should this right to a communicational personality become an inalienable right that cannot be removed. Electronic signatures and email addresses should therefore be available

on an affordable and long-term basis, irrevocable and protected against discriminating uses.

Traces

Already now when we are drafting our legislation on electronic signatures we should not only reflect on the validity of such signatures but we should become aware that increasingly such signatures will become a proof of and a necessity of our electronic existence. The conditions of acquiring and losing such a status will become as essential as - sometimes unfortunately - the proof of citizenship is becoming in our societies.

2.1.3 The right of access to information

Concept

Communicational inclusion does not exist for itself; it has a purpose: the purpose to know what is happening about us in more and more intangible environments, to know of which procedures we are becoming part of, what is happening in our communities, who is making which decisions on which assumptions. The right of inclusion comprises the right of access to information. The term access, however, will have to acquire a broader meaning: It will have to comprise to take possession of meaningful informational content, including advice if necessary, on which we ourselves then can base our decisions.

Traces

Freedom of information laws have been around for quite some time and they are slowly progressing in geographical scope and in depth as to which information is becoming available. The right is entering the electronic sphere, as the right to know about the contents of one's own personal files or the right to access electronic archives. There are already discussions to extend the concept of universal service to a universal service of information *content*. The most recent version of the EU Directive on Television without Frontiers bears witness of such an understanding.

2.1.4 The right to communicational participation

Concept

Getting access to information is always only a pre-step: In the total communication environment information rights have to lead to participatory rights and these rights have to be lifted to the level of available technology to let, wherever possible, information, commu-

nication and participation get fully integrated for more efficient and more meaningful citizenship. The right to communicational participation therefore requires adaptation of the technical tools of participation to the level of our time. Electronic democracy will have to supplement ever increasing electronic administration.

Extension

But this right is not only about "modernizing" forms of participation; the field of participation has also to be extended. We have already shown the importance of getting connected to a universal service of communication. The importance of this infrastructure and its high complexity demand a closer and less mediated involvement in the building of our communicational infrastructure. Europe in particular will need to reflect on models to involve individual citizens more directly in the design and building of their local, regional, national and transnational communication infrastructures, learning perhaps from models for public utilities in North America.

2.2 Rights to Communicational Exclusion

Communication, in our societies, is not only regarded as a necessity but as a choice, as a freedom. The right to inclusion therefore brings with it the right to freely chosen exclusion.

2.2.1 The right to privacy

The right to privacy, in as far as its defensive elements are concerned, is an expression of this right to remain excluded at one's own will, the right to be left alone. This right, however, will need further improvement as a right to remain excluded without being excluded from essential services. This means that we should resist the temptation to make the delivery of services increasingly dependent on payment by personal information and calling the result information processing with the consent of the individual. The reclusive side of the privacy right has to be strengthened so as to make such practices less and less acceptable.

2.2.2 The right to anonymity

Concept

Restrictions on the use of data might come too late or may not be sufficiently controllable. Personal information in the total communication environment should therefore be collected as sparingly as possible. In our everyday exchanges we have become used to a multitude of exchanges where we do not need personal data and still can perfectly interact with each other. We might remember situations where anonymity was even the prerequisite to

personal exchange. Anonymity therefore is an asset we should save into the total communication environment especially because of the totality this environment seeks to acquire.

Traces

There are already several regulations all over Europe that require e.g. that users should have the possibility to use pseudonyms in their communicational explorations. The European Directive on Telecommunications Privacy transfers some of the rules of anonymous social exchanges into the world of digital telephony. The debate about cryptography is also, partly at least, a debate on the right to anonymity.

2.2.3 The right to non-availability

Concept

One of the effects of the total communication environment in which we currently may indulge in because this effect seems to prove our personal importance is our increasing availability. In a total communication environment we become totally available or at least the social pressure will significantly increase to become and to remain totally available. In relations of dependency, not only within the family but also between the employer and the employee, it will become important to be able to require without the fear of sanctions the right *not* to be available.

2.2.4 The right to user empowerment

Concept

Finally, in the total communication environment there should be the right to be empowered to exclude oneself from information content. With cultural variety increases the risk to be by chance or deliberately exposed to material which with or without malicious intent may affect one's identity and integrity. At the same time, however, because of the importance of information, the simple choice "to switch it off" is no longer a simple choice. What is needed therefore is education and the availability of additional, selective defensive mechanism as they are beginning to be provided e.g. in the form of filters; they also help to defend oneself against the barrage of email spams. Such filters, however, due to their potential impact, should always remain transparent to their legitimate users and they should always be freely chosen.

2.3 Intermediate Summary

The right to communicational *inclusion* I have described as comprising

a) the right of access to the means of communication,

b) the right to an electronic or digital personality, inalienable as a citizenship,

c) the right of access to meaningful information, and

d) the right of access to communicational participation, both with regard to the means and the subject of communication.

The right of communicational *exclusion* I have shown as consisting of

a) the reclusive elements of the right to privacy,

b) the right to anonymity,

c) the right to non-availability and

d) the right to be empowered to manage information content on one's own.

Tensions

But rights do not stand alone. They may stand against each other. They demand balancing among themselves, with other more traditional rights. This then will remain the every day task of politics and law in the Informational Society. However, let me emphasize two sorts of tensions that will become increasingly important and that we will have to master for the future of our communicational societies.

Inclusion vs. property

The main conflict for communicational *inclusion* will be the conflict with property rights. Already we see the signs: How should a universal service be financed? Should we reformat the exemptions to intellectual property rights that in reaction to digitalization seem to move more and more into the formerly free areas of ideas and facts? Both examples, I am afraid, are but the expression of a more general uneasiness which we will have to face: the ethical future not only of our information societies but of our economic systems.

Exclusion vs. public interest

The main conflicts I see for communicational *exclusion* will be with public interests that may demand to refuse exclusion, to keep control. We witness this conflict e.g. in the current debate on cryptography.
These conflicts lead me to the issue of new responsibilities.

3. Responsibilities

3.1 Responsibilities as mirror images of rights

Mirror images

Have I used too much time on rights instead of giving rights and responsibilities an equal share? Talking about rights, so I feel, I have already talked about responsibilities: Responsibilities are mirror images of rights for those who need to advocate, to implement and when implemented to follow these rights.

In this respect these two types of rights will have one significant quality in common: They will no longer only be directed against the state, relevant only in the citizen-state relationship. They will become horizontal rights and thus horizontal responsibilities. Wherever the state is retreating or made to retreat those who step in its place will have to assume these responsibilities to make these rights work. This is an enormous task business organizations will have to face. In the interest of the coherence of our societies rights are meant to bridge differences in power, and responsibilities will need to be taken wherever these differences occur.

3.2 New responsibilities

New responsibilities

But beyond these mirror images of rights as responsibilities I see arise, just as new rights emerging from already existing rights, new responsibilities that take on a sharper image, that move into the forefront of our informational societies. I see these responsibilities grow on three levels: the individual - micro - level, the mezzo level and the macro level.

3.2.1 Micro level responsibilities

On the micro level, with regard to the role of the individual, what will increase is his and her communicational responsibility; a responsibility newspapers used to claim when they emphasized all the news that were fit to print. With the empowerment of the individual to participate in one-to-all, or at least one-to many structures of communication there should rise the awareness that messages have impacts, and in these environments not all impacts can be foreseen. This should lead - perhaps not to self-restraint - this sounds too puritan to me - but to some sort of communication environment consciousness: Basic rules that used to be valuable in direct communication will have to remain valid in the new forms of mediated communication. So the individual should remain aware of information quality, timeliness, correctness and context and the many meanings information may develop in different cultural environments.

3.2.2 Mezzo level responsibilities

What immediately comes to mind when addressing responsibilities on the mezzo level in the total communication environment is the issue of responsibility of information providers for illegal and harmful content. I feel, however, that this is not necessarily a new responsibility, and if it is a new responsibility we are quickly reaching at least a European consensus. The issue had received some attention because in the uncertainty of the evolving Internet the provider was the least mobile target for holding at least someone responsible, the author not being identifiable, or if identifiable not reachable for the law. The solution that emerged from the Bonn International Ministerial Conference in July last year, a solution that is also reflected e.g. in the German Multimedia Law and in the "Codice di autoregolamentazione per i servizi Internet" here in Italy:

First of all, as to contents providers, to be on-line is not a privilege, and what is against the law off-line is also against the law on-line.

Secondly, mere access providers, however, should only be held responsible if they have positive knowledge and if knowingly they did not change the situation, although - with reasonable efforts - they would have been able to do so.

With this approach the solution remains firmly on the basis of European general criminal law responsibility and avoids to create discrimination against organizations which have proved to be so vital for the use of these technologies.

3.2.3 Macro level responsibilities

The most difficult responsibility, however, in my opinion, occurs on the macro level, not only for the state as such, but for all that are involved in the rule making processes. It is the responsibility to adequately meet the challenge of anxiety. It is not only that change causes anxiety. The anxiety in the total communication environment is a very distinct anxiety. Communication invites. But every invitation is a challenge. So communication challenges, our values, our beliefs, our certainty, our identity. We tend to react with nervous anxiety against these challenges, a nervous anxiety that is a close neighbor to refusal, to rejection and if we are less trained to manage our feelings to violence. The most important task we have to learn in the total communication environment is the ability to sustain this challenge of communication, to persevere challenges to our identity.

This is a difficult task for an individual; it is extremely difficult for a society. And those involved in rule making should indeed take this anxiety seriously, but they should also at least not try to facilitate this painful learning process by too easy answers to those anxieties. This is the other side of communicational globalization: It is exposing us not so much to *the* global culture, such a thing might indeed be emerging, but first of all it is exposing us globally to globally different cultures.

4. Perspective

We are moving from human and civil rights which developed at the end of feudalism, to social rights which evolved with the height of industrialization toward informational and communicational rights which mark the turn from the industrial to the informational society. Not all the rights from the previous phases are yet fully accepted, and where accepted implemented, and where implemented always followed.

Social rights still fight for universal recognition let alone effective implementation. Informational and communicational rights, in most cases nothing but human, civil and social rights with a new specific emphasis, an emphasis for which the new technologies opened our eyes, will have an equally uneasy future.

The difference is, we know about them while we are entering the informational society. And if we know and if we can reasonably be expected to do something about them, then we are responsible to do something about them.

DIRITTI E RESPONSABILITÀ

Herbert Burkert

1. Introduzione

Viviamo in società vecchie dotate di nuove tecnologie. Come possiamo scoprire quando, dove e in che modo queste tecnologie potranno modificare la rete di vecchi diritti e responsabilità entro cui si svolge la nostra esistenza? Non v'è dubbio che un mutamento vi sarà, ma dovremmo metterlo in atto con l'aiuto dei nostri sistemi di diritto? A questi interrogativi basilari sul ruolo del diritto nella società dell'informazione (per usare il termine coniato da Manuel Castell) si può rispondere in molti modi. Una risposta possibile è che le nuove tecnologie incorporano sempre sogni sulla società ideale, mentre le leggi in esistenza rappresentano sempre compromessi politici congelati risalenti a momenti storici ben precisi.

Le nuove tecnologie tendono a "scongelare" questi compromessi e legittimano il dibattito sul cambiamento. La natura di tale cambiamento è strettamente legata al nucleo fondamentale di novità che si ritiene associato alle nuove tecnologie. A mio giudizio, questo nucleo innovativo è rappresentato dalla creazione di un "ambiente della comunicazione totale".

In questo ambiente è tecnicamente possibile per ogni individuo entrare in contatto con ogni altro individuo, attraverso qualsiasi supporto - suono, vista, anche tatto - e al di là di ogni barriera di tempo, spazio, complessità e cultura. Parlo di ambiente della comunicazio-

ne *totale* in quanto tutti gli atti comunicativi - con la stessa facilità - possono divenire essi stessi oggetto di comunicazione per gli scopi più diversi.

Ciò pone un problema fondamentale: la tecnologia aumenta il potere in misura esponenziale, pertanto quella che ho descritto come una *possibilità* per i singoli è invece una *certezza* per le varie organizzazioni. Nell'interesse della coesione sociale, caratterizzata dalla compresenza di interessi più o meno organizzati, occorre colmare tale divario, ed è in questo ambito che dovranno entrare in giuoco nuovi diritti e nuove responsabilità - che, come vedremo, non sono poi così nuovi, in ultima analisi.

2. Diritti

Mi pare che siano due le categorie fondamentali di diritti emergenti, dei quali già si rinviene traccia nei nostri sistemi giuridici:

- il diritto ad essere inclusi nelle comunicazioni, e
- il diritto ad essere esclusi dalle comunicazioni.

2.1. Il diritto ad essere inclusi nelle comunicazioni

Esso comprende in primo luogo:

2.1.1. Il diritto di accesso ai mezzi di comunicazione - Si tratta di un diritto dalle molteplici sfaccettature. In un ambiente di comunicazione totale, per partecipare alla ricerca della felicità, godersi le proprie libertà ed intervenire nei destini della comunità in cui si vive bisogna avere accesso ai *mezzi* di comunicazione e alla conoscenza delle modalità di utilizzo. Il diritto di accedere ai mezzi di comunicazione secondo modalità praticabili rappresenta dunque una delle componenti fondamentali del diritto ad essere inclusi nelle comunicazioni.

Troviamo le prime tracce di questo diritto in evoluzione nel concetto di servizio universale riferito alla normativa in materia di telecomunicazioni.

2.1.2. Il diritto alla personalità comunicativa - Nell'ambiente della comunicazione totale comunicheremo sotto forma di repliche mediatiche di noi stessi. Possedere e controllare tali repliche diverrà fondamentale per partecipare agli scambi commerciali, per comunicare con le autorità, per esercitare i diritti civili ed anche per rimanere in contatto con famiglie e amici. La firma elettronica e l'indirizzo e-mail sono esempi di tali repliche attraverso le quali esistiamo nell'ambiente della comunicazione totale. Quanto più esteso sarà questo ambiente, tanto più indispensabili diverranno le repliche elettroniche di cui parlavamo. Le repliche elettroniche diverranno espressione fondamentale del fatto di essere un individuo dotato di personalità giuridica. Così come non è possibile abolire completamente tale personalità, allo stesso modo questo diritto ad una personalità comunicativa dovrebbe divenire un diritto inalienabile e ineliminabile. Pertanto, firma elettronica e indirizzo e-mail dovreb-

bero essere disponibili secondo criteri di accessibilità, nel lungo periodo, in modo irrevocabile e tutelato nei confronti di utilizzi discriminatori.

Già oggi, nello scrivere la legislazione sulla firma elettronica, dovremmo non soltanto riflettere sulla validità di tali firme, ma anche renderci conto che esse diverranno in misura crescente prova e necessità della nostra esistenza elettronica. Le condizioni di acquisto e perdita di tale personalità diverranno fondamentali così come - per alcuni versi, purtroppo - lo è sempre più la possibilità di dimostrare la propria cittadinanza.

2.1.3. Il diritto di accesso alle informazioni - L'inclusione comunicazionale non esiste in quanto tale: ha uno scopo, quello di sapere cosa succede intorno a noi in ambienti sempre più intangibili, sapere di quali procedure diveniamo parte, cosa succede nella comunità cui apparteniamo, chi decide, quali decisioni vengono prese e sulla base di quali presupposti. Il diritto di inclusione comprende anche il diritto di accesso alle informazioni. Tuttavia, bisognerà attribuire al termine "accesso" una valenza più ampia: esso dovà comprendere il fatto di entrare in possesso di contenuti informazionali significativi (anche di natura consultiva) sui quali basare successivamente le nostre decisioni.

La legislazione in materia di libertà di informazione esiste da tempo, ed è in atto una lenta evoluzione in termini di ambito geografico e di entità delle informazioni disponibili. Il diritto entra nella sfera elettronica, come nel caso del diritto di conoscere il contenuto dei fascicoli personali che ci riguardano o il diritto di accedere ad archivi elettronici. Già si parla di ampliare il concetto di servizio universale ad un servizio universale in termini di contenuti informativi. E' un orientamento testimoniato anche dall'ultima versione della Direttiva UE sulla televisione senza frontiere.

2.1.4. Il diritto di partecipare alla comunicazione - Accedere alle informazioni è soltanto un passo preliminare. Nell'ambiente della comunicazione totale i diritti dell'informazione devono condurre ai diritti della partecipazione, e questi ultimi devono essere sollevati al livello della tecnologia disponibile per consentire, nei limiti del possibile, la piena integrazione di informazioni, comunicazione e partecipazione in modo da conferire più efficienza e significatività alla condizione di cittadino. Dunque, il diritto di partecipare alla comunicazione impone di adeguare gli strumenti di partecipazione al livello contemporaneo. La democrazia elettronica dovrà integrare l'amministrazione gestita in misura crescente su base elettronica.

Non si tratta però semplicemente di "modernizzare" le forme di partecipazione: occorre inoltre ampliare l'*ambito* di partecipazione. Abbiamo già mostrato l'importanza di collegarsi ad un servizio universale di comunicazione. L'importanza di tale infrastruttura e al contempo la sua elevata complessità impongono una partecipazione più ravvicinata e meno mediata alla sua costruzione. L'Europa, in particolare, dovrà elaborare modelli utili a realizzare il coinvolgimento dei singoli cittadini nella definizione e nella costruzione delle rispettive infrastrutture comunicative di livello locale, regionale, nazionale e transnazionale - magari imparando dai modelli adottati per i servizi pubblici in Canada e negli USA.

2.2. Il diritto ad essere esclusi dalle comunicazioni

Nella nostra società la comunicazione non è considerata soltanto una necessità, ma anche una scelta - una libertà. Dunque, il diritto ad essere inclusi nelle comunicazioni comporta anche il diritto di scegliere liberamente di esserne esclusi.

2.2.1. Il diritto alla riservatezza - Il diritto alla riservatezza, per quanto riguarda gli aspetti difensivi che lo caratterizzano, è espressione di questo diritto ad essere esclusi sulla base di una libera scelta, il diritto ad essere lasciati in pace. Tuttavia, occorrerà migliorare ulteriormente tale diritto facendone un diritto ad essere esclusi senza però essere esclusi da servizi essenziali. Ciò significa che dovremmo resistere alla tentazione di subordinare in misura crescente la prestazione di servizi al pagamento attraverso informazioni personali, chiamando il risultato "trattamento dati con il consenso dell'interessato". Occorre potenziare il lato "eremitico" del diritto alla riservatezza, in modo da rendere sempre meno accettabili pratiche di questo tipo.

2.2.2. Il diritto all'anonimato - Le limitazioni all'utilizzo dei dati potrebbero giungere troppo tardi, o magari non essere sufficientemente controllabili. Pertanto, la raccolta di dati personali dovrebbe avvenire con la massima parsimonia nell'ambiente della comunicazione totale. Nelle interazioni quotidiane siamo abituati a molte circostanze in cui, senza bisogno di dati personali, possiamo comunque interagire perfettamente. In alcuni casi l'anonimato rappresenta addirittura un prerequisito per lo scambio personale. L'anonimato costituisce dunque un patrimonio da tutelare nell'ambiente della comunicazione totale, soprattutto per la totalità che questo ambiente mira ad acquisire.
A livello europeo esistono già varie disposizioni di legge che, ad esempio, prevedono per gli utenti la possibilità di ricorrere a pseudonimi nelle esplorazioni comunicative. La Direttiva europea sulla privacy nelle telecomunicazioni trasferisce al mondo della telefonia digitale alcune delle regole proprie delle interazioni sociali anonime. Il dibattito sulla crittografia è, almeno in parte, anche un dibattito sul diritto all'anonimato.

2.2.3. Il diritto alla non raggiungibilità - Uno degli effetti dell'ambiente della comunicazione totale, in cui rischiamo di indulgere perché sembra offrire la prova della nostra personale importanza è la crescente raggiungibilità. In un ambiente della comunicazione totale la raggiungibilità di ciascuno di noi diviene totale, o quanto meno si assisterà ad un aumento significativo della pressione sociale tesa a realizzare e mantenere una raggiungibilità totale. Nell'ambito dei rapporti di dipendenza, non solo in seno alla famiglia, ma anche fra datore di lavoro e lavoratore, sarà sempre più importante poter rivendicare il diritto a *non* essere raggiungibili senza dover temere sanzioni.

2.2.4. Il diritto dell'utente di avere la possibilità di scegliere - Infine, nell'ambiente della comunicazione totale dovrebbe esistere il diritto di avere la possibilità di autoescludersi dai

contenuti informazionali. Con la varietà culturale aumenta il rischio di venire esposti, casualmente o volontariamente, a materiali che possono riflettersi negativamente sulla propria identità e integrità, su base dolosa o meno. Allo stesso tempo, tuttavia, data l'importanza delle informazioni, la semplice scelta di "spegnere" non è più una scelta semplice. Pertanto, c'è bisogno di educare e di introdurre altri meccanismi selettivi di difesa sul modello di quelli che iniziano ad essere disponibili sotto forma, ad esempio, di filtri; questi ultimi aiutano anche a difendersi dal fuoco di sbarramento dei messaggi di posta elettronica indesiderati. Tuttavia, dato il loro impatto potenziale, filtri del genere dovrebbero rimanere sempre trasparenti per i rispettivi utenti legittimi, ed il loro utilizzo dovrebbe essere frutto di una libera scelta.

2.3. Sintesi intermedia

Il diritto ad essere *inclusi* nelle comunicazioni comprende, secondo quanto prima indicato:

a) il diritto di accesso ai mezzi di comunicazione;

b) il diritto ad una personalità elettronica o digitale, inalienabile allo stesso modo della cittadinanza;

c) il diritto di accedere ad informazioni significative, e

d) il diritto di partecipare alla comunicazione per quanto riguarda sia gli strumenti sia l'oggetto di tale comunicazione.

Il diritto ad essere *esclusi* dalle comunicazioni comprende invece, secondo quanto prima indicato:

a) gli elementi "eremitici" del diritto alla riservatezza;

b) il diritto all'anonimato;

c) il diritto alla non raggiungibilità, e

d) il diritto di avere la possibilità di gestire in modo autonomo i contenuti informazionali.

Tuttavia, i diritti non esistono in forma isolata: possono anche essere reciprocamente in contrasto. Impongono un bilanciamento anche rispetto ad altri diritti più tradizionali. Questo è il compito che rimane da svolgere alla politica e al diritto nella società dell'informazione. Vorrei però sottolineare due situazioni conflittuali che acquisteranno importanza crescente e che dovremo essere in grado di gestire per il futuro delle nostre società della comunicazione.

Il conflitto primario per quanto riguarda l'*inclusione* nell'ambito comunicativo sarà quello con i diritti di proprietà. Ne possiamo già scorgere le prime avvisaglie: come finanziare un servizio universale? È necessario riformulare le eccezioni ai diritti di proprietà intellettuale che, per reazione alla digitalizzazione, sembrano spostarsi sempre di più verso le aree un tempo libere delle idee e dei fatti? Temo che entrambi gli esempi siano solo l'espressione di un disagio più generale con cui dovremo fare i conti: il futuro etico non soltanto della società dell'informazione, ma dei nostri sistemi economici in genere.

Il conflitto principale per quanto riguarda l'*esclusione* dall'ambito comunicativo ritengo che si focalizzerà sugli interessi pubblici che possono imporre di negare l'esclusione, di mantenere il controllo. È un conflitto visibile, ad esempio, nel dibattito in corso sulla crittografia. Arriviamo così al tema delle nuove responsabilità.

3. Responsabilità

3.1. Le responsabilità come immagine speculare dei diritti

Mi sono dilungato eccessivamente sui diritti, senza dare pari spazio al tema delle responsabilità? Parlando di diritti, credo di avere già affrontato il tema delle responsabilità. Le responsabilità sono immagini speculari dei diritti per chi deve difendere, attuare e, una volta attuati, seguire tali diritti.

In questo senso le due categorie di diritti di cui abbiamo parlato avranno una caratteristica significativa in comune: non saranno più rivolti esclusivamente contro lo Stato, non avranno più attinenza esclusivamente con il rapporto cittadini-Stato. Diverranno diritti orizzontali, e si avranno dunque responsabilità orizzontali. Dovunque lo Stato si fa da parte o viene costretto a farsi da parte, chi gli subentra dovrà farsi carico di tali responsabilità per dare realizzazione ai diritti. Si tratta di un compito immane che attende gli organismi del settore imprenditoriale. Nell'interesse della coerenza delle nostre società, i diritti servono a colmare differenze in termini di potere, ed occorrerà farsi carico di determinate responsabilità ogniqualvolta si manifestino differenze del genere.

3.2. Nuove responsabilità

Tuttavia, al di là di questa specularità dei diritti *in quanto* responsabilità, vedo emergere, accanto ai nuovi diritti che nascono da diritti già esistenti, nuove responsabilità che acquistano un profilo più netto, che passano in prima linea nella società dell'informazione. Vedo queste responsabilità crescere a tre diversi livelli: il singolo, ossia il micro-livello, un livello intermedio ed un macro-livello.

3.2.1. Responsabilità di micro-livello - Al micro-livello, relativo al ruolo del singolo, quello che è destinato a crescere è la responsabilità comunicativa, una responsabilità cui la stampa era solita fare riferimento nell'enfatizzare tutte le notizie *passibili* di pubblicazione.

Con la possibilità per i singoli di partecipare a strutture comunicative in cui l'individuo è in rapporto con tutti gli altri soggetti della comunicazione, o almeno con molti di tali soggetti, dovrebbe manifestarsi anche la consapevolezza dell'impatto del messaggio, e in questi ambienti non sempre l'impatto è prevedibile. Tutto ciò dovrebbe portare, non dico ad una sorta di auto-limitazione - un termine che mi sembra eccessivamente puritano -, ma ad una forma di coscienza dell'ambiente della comunicazione. I principi fondamentali validi per la comunicazione diretta dovranno restare validi nelle nuove forme di comunicazione

mediata. Il singolo dovrebbe dunque mantenere la consapevolezza della qualità, della puntualità, della correttezza e del contesto delle informazioni, e della molteplicità di significati che la stessa informazione può assumere entro contesti culturali diversi.

3.2.2. Responsabilità di livello intermedio - Quello che viene subito in mente passando all'esame delle responsabilità di livello intermedio nell'ambiente della comunicazione totale è la responsabilità dei fornitori di informazioni rispetto ai contenuti illeciti e dannosi. Ho l'impressione, tuttavia, che non si tratti necessariamente di una responsabilità del tutto nuova, e se anche lo fosse stiamo comunque avvicinandoci ad una posizione comune almeno a livello europeo. Il tema era già stato affrontato, poiché nell'incertezza che caratterizzava lo sviluppo di Internet il fornitore rappresentava il bersaglio meno mobile nell'individuazione di responsabilità, dato che l'autore non è identificabile o, se lo è, non è alla portata della legge. La soluzione emersa dalla Conferenza ministeriale internazionale tenutasi a Bonn nel luglio dello scorso anno, e che ha trovato echi, ad esempio, nella Legge tedesca sulla multimedialità e nel "Codice di autoregolamentazione per i servizi Internet" in Italia, è la seguente:

In primo luogo, per quanto riguarda i fornitori di contenuti, il fatto di trovarsi on-line non costituisce un privilegio, e quello che è illegale off-line lo è anche on-line.
In secondo luogo, i fornitori di accesso dovrebbero essere ritenuti responsabili soltanto se sono effettivamente a conoscenza della situazione e scientemente non intervengono per modificarla, pur avendone avuto la possibilità mettendo in atto uno sforzo ragionevole.
Con questo approccio, la soluzione resta fermamente ancorata al concetto di responsabilità generica secondo il diritto penale europeo, e si evita ogni discriminazione nei confronti di soggetti che si sono dimostrati fondamentali per l'utilizzo delle tecnologie in questione.

3.2.3. Responsabilità di macrolivello - Le responsabilità più gravose sono comunque, a mio giudizio, quelle di macro-livello. Non soltanto per quanto riguarda lo Stato in quanto tale, ma anche per tutti i soggetti che partecipano al processo di normazione. Si tratta della responsabilità di dare una risposta adeguata all'angoscia. Il problema non è semplicemente che ogni cambiamento provoca angoscia. L'angoscia dell'ambiente della comunicazione totale è un'angoscia molto particolare. La comunicazione costituisce un invito, ma ogni invito è anche una sfida. Per questo la comunicazione mette in discussione i nostri valori, le nostre convinzioni e certezze, la nostra identità. Tendiamo a reagire a questa sfida sviluppando un'angoscia nervosa - molto vicina al rifiuto, al rigetto, e, se siamo meno abituati a gestire le reazioni emotive, alla violenza. L'abilità più importante che dobbiamo acquisire nell'ambiente della comunicazione totale è quella di sostenere questa sfida comunicativa, perseverare nell'accogliere ogni sfida alla nostra identità. E' un compito difficile per il singolo, ed è estremamente difficile per la società. Ed i soggetti che partecipano al processo di normazione dovrebbero prendere sul serio questa angoscia, ma dovrebbero anche evitare quantomeno di facilitare questo doloroso processo di apprendimento fornendo risposte troppo facili alle angosce di cui si diceva. Questa è l'altra faccia della globalizzazione comunicativa. Ci espone non tanto a *la* cultura globale, che potrebbe essere un realtà o meno,

bensì, e in primo luogo, ci espone globalmente a culture globalmente diverse.

4. Prospettive

È in atto un processo di transizione che dai diritti civili e dell'uomo, sviluppatisi alla fine dell'era feudale, conduce ai diritti sociali, la cui definizione ha coinciso con l'apogeo della rivoluzione industriale, puntando verso i diritti dell'informazione e della comunicazione che segnano il passaggio dalla società industriale alla società dell'informazione. Non tutti i diritti derivanti dalle fasi precedenti trovano ancora pieno accoglimento, né ove accolti vengono pienamente attuati, né ove attuati vengono sempre seguiti.

Ancora si combatte per dare ai diritti sociali un riconoscimento universale, per non parlare di un'effettiva attuazione. Un futuro egualmente incerto attende i diritti dell'informazione e della comunicazione - che nella maggioranza dei casi sono i diritti dell'uomo, i diritti civili e sociali con un accento più specifico nei cui confronti le nuove tecnologie ci hanno aperto gli occhi.

La differenza consiste in questo: che ne abbiamo coscienza mentre facciamo il nostro ingresso nella società dell'informazione. E se abbiamo questa consapevolezza e se è ragionevole pensare di essere tenuti ad agire in rapporto a questi diritti, allora abbiamo la responsabilità di agire.

Cons. Giovanni Buttarelli

Con l'intelligenza ed il talento che lo contraddistingue, Herbert Burkert ha immesso in rete una serie di concetti che non è facile riassumere e che forse, lungi dall'essere generali o generici, implicano una riflessione che probabilmente non potrà neanche esaurirsi oggi. Una serie di categorie che impongono una riflessione proprio per quelle macro-level responsibilities che ha citato per ultime e che sono certamente oggetto di riflessione, perché poi, scelte sbagliate dopo un dibattito così approfondito possono veramente creare problemi.

Desidero solo ricordare dell'intervento di Burkert un aspetto, che per la verità anche ieri era emerso nel corso dei lavori, che il diritto dell'utente di non lasciare tracce in rete superflue o di non essere penalizzato dal fatto di dover lasciare tracce, non può poi ripercuotersi a suo danno, con una penalizzazione rispetto alla possibilità di essere un cittadino elettronico e di usufruire di una serie di servizi.

L'attenzione si sposta forse sul secondo dei temi di oggi: diritti e responsabilità, sull'aspetto delle responsabilità, perché diamo la parola a Marco Barbuti che è qui non soltanto nelle vesti di amministratore delegato di un importante provider italiano - Italia Online - ma piuttosto come presidente dell'Associazione Italiana degli Internet Provider, impegnata molto anche in collegamento con le omologhe associazioni in ambito europeo per l'approfondimento delle tematiche che riguardano l'aspetto soprattutto deontologico.

Al dott. Barbuti, oltre agli stimoli che sono venuti in apertura di sessione, mi permetto di aggiungere un ulteriore stimolo, che riguarda specificamente i *Provider*, ed è una *Privacy Policy Chart*, di cui parlavamo poc'anzi, che in realtà è uno studio delle pratiche osservate dai maggiori *Service Providers* negli Stati Uniti.

Questo documento, che è reperibile in rete, si articola in 26 domande che sono state poste da alcuni ricercatori ai quattro principali *Provider* americani. Si chiede loro come si comportino rispetto alla *privacy* degli utenti, come conservino la posta elettronica, le cosiddette "testatine", i *log* delle transazioni, come regolino l'informativa; poi vi sono tutta una serie di "yes" o "no", ed il documento, nel suo insieme, è molto articolato.

Non è certo il caso di entrare nei dettagli, e ritengo che questo documento sia soltanto utile considerarlo per il fatto che emerge una prassi nettamente diversa, su aspetti che però costituiscono un punto fondamentale, e cioè che incidono veramente ed effettivamente sulla vita privata delle persone.

Noi ci chiediamo come si possa fare, in futuro, per armonizzare questo tipo di prassi, per fare in modo che la legittima concorrenza tra *Providers* sia un conto, e che però le prassi che più direttamente riguardano la vita privata delle persone possano essere armonizzate nel modo più flessibile e, forse, dal basso possibile.

Dr. Marco Barbuti
Presidente AIIP - Associazione Italiana Internet Provider

Desidero anzitutto ringraziare la struttura del Garante per la protezione dei dati personali per l'ottimo lavoro fatto per la preparazione di questo evento così importante; ringrazio il Presidente, professor Rodotà, per l'invito e, oltre che a nome mio personale, ringrazio a nome della A.I.I.P., l'Associazione italiana Internet Providers, e in generale della categoria degli ISP italiani.

Anche se l'Internet che conosciamo è frutto dell'esplosione di massa di questi ultimi anni, il settore è composto da operatori che hanno esperienza nella Rete che risale anche a oltre dieci anni di attività, inoltre in Italia oggi vi sono più di trecento Internet Provider, a nome dei quali vorrei proporre alla vostra attenzione alcune istanze e dare possibilmente delle risposte alle numerosissime questioni sollevate nel corso di questo incontro.

Occorre anzitutto sottolineare che l'A.I.I.P. è presente in diverse sedi istituzionali internazionali per far sì che si arrivi a meglio definire il quadro normativo e di autoregolamentazione relativo a Internet. Siamo presenti per esempio in EuroISPA, l'Associazione europea delle Associazioni di Internet Provider, alla quale aderiscono nove Paesi europei, e tramite questa siamo presenti alla Commissione Europea ed al Consiglio d'Europa, che si occupa tra l' altro degli aspetti relativi al servizio universale, a cui il dottor Burkert ha fatto cenno; siamo inoltre presenti presso l'OCSE, dove ci occupiamo non solo di autoregolamentazione, ma anche di crittografia, di registrazione di domìni, di commercio elettronico e così via.

In primo luogo vorrei parlare del mercato che Internet rappresenta in Italia. Noi operatori abbiamo avuto modo di constatare che Internet in Italia, per quanto sconti il tradizionale ritardo tecnologico, sta esplodendo e crescendo ad una velocità molto superiore rispetto agli altri Paesi dell'America e dell'Europa, e quindi riteniamo vi sia la possibilità di recuperare almeno parte del terreno perduto. Sulla base dei dati in nostro possesso, in particolare quelli forniti da EURISKO e CENSIS, si desume che ormai la penetrazione del PC nelle famiglie raggiunge il 25 per cento, una percentuale che si avvicina ormai alle medie europee.

EURISKO e ALCHERA ci dicono inoltre che coloro che in qualche modo hanno accesso alla rete, erano stimati in 1.800.000-2.400.000 alla fine del '97. Si tratta di una percentuale di penetrazione ancora inferiore rispetto alle medie europee, ma analizzando l' evoluzione degli altri principali indicatori del settore Internet, constatiamo tassi di crescita del 100 per cento ogni 6-8, massimo 12 mesi, a seconda dei fenomeni osservati. In particolare, il numero di abbonati residenziali a Internet (le famiglie collegate) è stato stimato a fine 1997 in 300.000 unità, ma la previsione per fine 1998 è di 7-800.000.

Il fenomeno si evidenzia in modo particolare se si considera lo sviluppo dei siti su Internet.

Oggi tutti i più importanti siti con contenuti italiani cominciano a sviluppare contatti

importanti, dell'ordine dei 10 milioni di contatti al mese. Comincia ad essere un volume di attività corposo, un gruppo sociale rilevante, ed anche, ovviamente, un mercato da tenere in considerazione dal punto di vista pubblicitario. Al di là di questi dati puntuali, ritengo siano evidenti la grande opportunità e la forte dinamica che oggi caratterizzano il mercato italiano.

In secondo luogo vorrei intervenire sul quadro generale delle problematiche tra Internet e privacy. A questo proposito, va notato che ci troviamo in perfetta sintonia con l'illustrazione data in apertura dal professor Rodotà, e perfettamente allineati sui vari temi, anche se occorrono alcune precisazioni. In particolare quando si parla ad esempio di tutela dell'anonimato, tutela che ci trova assolutamente concordi a condizione che si tratti di un anonimato protetto, ossia della riconoscibilità dell'operatore sulla rete.

Ancor più delicata è la questione della responsabilità dell'Internet Provider in tema di contenuti, allorchè constatiamo che l' estraneità del Provider rispetto ai contenuti immessi in rete da terzi non è così scontata, come abbiamo avuto modo di vedere ancora in questa sede; lo abbiamo sentito dal professor Rodotà ed è anche emerso dal quadro europeo che ci ha illustrato il dottor Burkert: che il Provider non possa conoscere tutto ciò che passa attraverso la propria rete, e non abbia mezzi per effettuare un controllo, è un dato di fatto. Non sarebbe possibile altrimenti.

Quindi, che qualcuno possa ipotizzare una responsabilità del gestore del traffico in relazione al contenuto immesso da terzi è un'assurdità, ma purtroppo non è una considerazione scontata. Infatti, si deve purtroppo constatare che addirittura l'On.le Veltroni, sicuramente in buona fede, ha citato il caso, ancora purtroppo ambiguo, rappresentato dal disegno di legge in tema di tutela dei minori che sta per essere discusso alla Camera, in cui si cita in termini assai generici la responsabilità penale (con pene da uno a cinque anni) per tutti coloro che diffondono - anche per via telematica - contenuti che hanno a che fare con lo sfruttamento dei minori, senza individuare la responsabilità dell' autore e dell' eventuale distributore, e soprattutto senza chiarire l' estraneità di chi esercita un puro servizio di telecomunicazione.

In base a queste ambiguità, che rappresentano un fatto non banale, in Francia ed in Germania sono stati imputati alcuni Provider per fatti estranei alla loro possibilità di intervento. Vorremmo evitare che questo avvenisse anche in Italia, e quindi la mia preghiera è che su questi argomenti non secondari ci sia un approfondimento anche tecnico nelle dovute sedi normative.

Vi sono, in particolare, alcuni elementi che reputo importante valutare, e che sono stati citati, ad esempio, del professor Poullet, il quale ha illustrato come alcuni trattamenti dei dati della rete siano poco noti ed implichino il fatto che chi non ne conosce il traffico può essere oggetto di un controllo a sua insaputa. In particolare, è necessario capire meglio che cosa sono i cookies, o che cosa vuol dire mantenere o distruggere dei log files. E ci accorgeremo che, tutto sommato, non risiedono in questi elementi i problemi più seri per la tutela della privacy dell' utente.

I cookies, che pure ci sorprendono perché ci riconoscono quando entriamo in rete,

sono un fatto fondamentale e irrinunciabile del servizio. Il problema è come gestirli.

Quando infatti, in base ai cookies, l'utente Internet si profila, quindi fornisce i propri dati perché desidera sottoscrivere un servizio personalizzato, è chiaro che quei dati, come, del resto, tutti i dati che ciascuno di noi fornisce quando sottoscrive un abbonamento ad una rivista, possono essere oggetto di diffusione. Occorre dunque tenere sotto controllo il metodo di trattamento e di archiviazione di questi dati.

Ma quando parliamo di log files, che hanno la capacità di monitorare le nostre azioni sulla rete, va detto innanzitutto che per conoscere esattamente che cosa fa un operatore sulla rete, bisogna disporre contemporaneamente dei log file del Service Provider e dei log file del Content provider, per individuare quali contenuti siano stati visitati. Ma se non viene realizzata questa corrispondenza, non sarà possibile tracciare l'attività in rete dell'operatore.

Alcune facili soluzioni si traducono in proposte - ad esempio - di eliminare i cookies e, addirittura, di distruggere i log files dopo poche settimane, senza rendersi conto del fatto che se eliminiamo i cookies eliminiamo anche i servizi, e se distruggiamo i log files non saremo mai più in grado, ad esempio, di stabilire in seguito se c'è stata la violazione di una legge, se c'è stata un'offesa, se c'è stato un attentato sulla rete, non ne potremo rintracciare l'autore. E questa non è una banalità.

Ecco quindi che le soluzioni ai problemi di tutela della privacy devono essere il frutto di una conoscenza approfondita dei fenomeni e di una sensibilità sulle relazioni di causa ed effetto. Non possiamo prendere decisioni affrettate e generiche.

Prendendo spunto dall' intervento della professoressa Samuelson, dobbiamo rifarci al pragmatismo tipico statunitense secondo il quale, ad esempio in tema di proprietà intellettuale, bisogna saper gestire un equo bilanciamento tra l'esigenza della protezione dei diritti intellettuali, evitando però la cosiddetta over protection. Se vogliamo garantire infatti uno sviluppo tecnologico adeguato, dobbiamo saper bilanciare le esigenze di tutela dell'innovatore (dell'inventore), ma anche le esigenze del follower, che può in seguito creare valore aggiunto rispetto all' invenzione originale. In poche parole, occorre una conoscenza approfondita dei fenomeni e saper bilanciare gli interventi.

Vorrei quindi passare ad un terzo importante argomento che è stato solo vagamente citato e che, a nostro parere, è invece quello più importante. Si tratta della problematica cui ha fatto cenno il Commissario Europeo, Onorevole Bonino, quando ha brevemente illustrato quale sia sulla rete una minaccia più seria alla privacy.

Debbo dire che la più grande minaccia non è rappresentata dai cookies o dai log files.

La grande minaccia è stata descritta già da decenni, ed è l'orwelliano "*Grande Fratello*", ossia un grande *data base*, contenente tutte le informazioni, e non brandelli di informazioni, per cui si determini la possibilità di un controllo totale delle nostre attività.

La minaccia è che non si possa sfuggire a questo grande *data base*, si sia costretti a rimanere là dentro. Questa non è una banalità, perché in Italia vi sono rischi concreti, che illustrerò, di andare in questa direzione.

Consideriamo il nostro grande operatore di telecomunicazioni, quello che fino a ieri era un monopolio di telefonia e che da qualche mese è aperto alla liberalizzazione. Come

tutti i grossi monopoli, ha impiegato del tempo a capire il nuovo fenomeno, e nel nuovo mercato di Internet non è entrato fino a due anni fa. Il nuovo mercato stava esplodendo, 300 operatori sono nati, c'è voluto tempo perché il grande operatore si decidesse, ma poi, improvvisamente, ha deciso e ha acquisito l'operatore più grosso: Video Online.

E' bastato assaggiare il nuovo mercato per decidere che all' ex-monopolio non può bastare il 35 % di quota di mercato. Ed è tale la corsa a ricostituire il monopolio anche nel mercato libero di Internet che già oggi il grande operatore ha il 50 per cento di quota di mercato nell' accesso residenziale; negli ultimi sei mesi stimiamo che abbia raccolto il 65-70 % di tutti i nuovi abbonati.

Se si potesse dire che questa fenomenale rimonta è dovuta al fatto che il nuovo entrante (ma vecchio Incumbent) è l' operatore più efficiente non vi sarebbe nulla da eccepire, poiché nel libero mercato chi è più bravo guadagna quota di mercato.

Purtroppo le cose non stanno così: la quota di mercato dell'Incumbent che sta schiacciando ed uccidendo tutti i liberi operatori Internet in Italia, non solo nell'accesso, è conquistata attraverso azioni che riteniamo siano da valutare con attenzione perché potrebbero configurarsi come un chiaro esempio di concorrenza sleale, in particolare quando si dovesse constatare l'esercizio sul mercato di prezzi predatori di discriminazione della clientela e di sussidi incrociati che dovrebbero essere oggetto quindi di attenta vigilanza da parte degli organi ad essa preposti.

Tanto per fare un esempio, quando viene offerto agli studenti universitari l'accesso ad Internet con posta elettronica, con tutti i servizi connessi, a 150 mila lire l'anno (meno della metà dei prezzi USA, che pure hanno costi di telecomunicazione infinitamente più bassi che da noi), quando è evidente dall'esame dei bilanci (ricordiamo che l'Antitrust aveva a suo tempo imposto almeno la contabilità separata) che il prezzo di vendita è di gran lunga inferiore ai costi variabili per l'esercizio del servizio, non si configura una pratica di prezzi predatori?

In questo modo tra l'altro si fanno sicuramente felici nel breve termine gli studenti universitari, ma si creano i presupposti, di qui a uno-due anni, quando sarà stata raggiunta la condizione di monopolio, di fissare finalmente un prezzo che sarà allora commisurato al costo, costo peraltro di gran lunga superiore ai costi dei concorrenti.

Questo comportamento si declina tra l'altro in un'altra - parallela - pratica che riteniamo sia da osservare attentamente alla luce di possibile concorrenza sleale, in particolare in tema di discriminazione della clientela. Se si prendono in considerazione infatti le offerte di servizi agli Internet Provider, si può constatare che soltanto il servizio di accesso alla rete (il servizio Arcipelago ad esempio, che non comprende il servizio di banda internazionale ed il servizio di posta elettronica), viene venduto a 200-250 mila lire, un prezzo assai superiore al prezzo offerto all'utente finale per un servizio assai più completo e che normalmente ha costi tripli rispetto al puro accesso alla rete offerto all' ISP.

Un'altra pratica che merita di essere vagliata alla luce della disciplina della concorrenza è quella dei sussidi incrociati, che permettono di poter sostenere - sulla base del bilancio 1996, di cui noi abbiamo visibilità - ricavi dell'Incumbent sul mercato consumer di

Internet per 9 miliardi, a fronte di costi per 60 miliardi, vale a dire oltre 6 lire di costi per ogni lira incassata.

Ma non è finita qui, il nostro grande operatore non solo palesa l'obiettivo del monopolio dell'accesso alla rete, ma vuole anche fare in modo di prendere il completo controllo del resto dei servizi a valore aggiunto. Sta infatti investendo nelle piattaforme software, nelle soluzioni di system integration, nel commercio elettronico, nei sistemi abilitanti delle transazioni; addirittura si propone come certification authority, quell'organismo che ci darà la firma elettronica e le carte intelligenti.

Per comprendere quali e quante risorse possono essere dedicate dall'Incumbent al nuovo mercato, possiamo rifarci al caso emblematico di Stream, che in pochi anni ha consumato oltre 500 miliardi di lire investendo in esperimenti di Pay TV, Pay per View, Cable TV, Video On Demand, TV Sat, senza ad oggi aver costruito alcun serio servizio agli utenti, e per arrivare infine, sembra, ad essere interessata all'Internet TV.

Questa realtà, il rischio che sta correndo il settore nei confronti della libera concorrenza, deve essere affrontata e vanno trovate le opportune soluzioni, nelle sedi competenti, e anche piuttosto rapidamente. Non si tratta di assumere un atteggiamento contrario al nostro operatore nazionale di telecomunicazioni, anzi noi riteniamo che la nostra grande azienda nazionale vada sostenuta. Essa deve affrontare una concorrenza internazionale e globale, e proprio in questo deve essere sostenuta con politiche nazionali che ne garantiscano la competitività globale, ma dobbiamo evitare che Telecom perseveri il monopolio in Italia e in particolare evitare che lo riacquisti sull'Internet italiana.

Mi sembra di aver dimostrato che il problema è che quando tutti noi avessimo un unico operatore Internet, che non solo fosse in grado di possedere tutti i nostri log file di accesso, ma anche quelli del contenuto, e poi avesse le tracce delle nostre transazioni economiche, e quindi i nostri documenti elettronici, a quel punto avremmo prodotto il Grande Fratello, e allora ci troveremmo ad affrontare un serio problema di tutela della nostra privacy. Non è un evento poi così lontano, se si pensa che sull'accesso in pochi mesi si è passati dal 35 al 60-70 per cento di quota di mercato, e che le risorse straordinarie che ha questo operatore impediscono ai 300 piccoli provider di un mercato che ancora deve nascere, la possibilità di svilupparsi.

Questo è quindi il primario problema di privacy, che vorrei sottoporre a questa Autorità garante della protezione dei dati personali, problema che va gestito per garantire che la democrazia del cittadino sia anche possibilità di scelta tra diversi operatori. È vitale sapere che i nostri dati li ha oggi un operatore ma li può avere domani un altro, che i dati del nostro collega li ha un altro ancora, e che questi non stanno in un unico grande data base, di cui non abbiamo il controllo. Oggi tra l'altro siamo di fronte ad un operatore di telecomunicazioni che ormai non è più un operatore pubblico, ma è controllato da privati che possono acquisire una quota direttamente sul mercato di Borsa.

Mi avete permesso di spiegare questo nostro punto di vista e di precisare che non si tratta di un atteggiamento di contrasto con alcuno, ma siamo ispirati dalla volontà di far crescere questo settore così importante per lo sviluppo della società dell' informazione

Arrivo ora al punto che abbiamo trattato più volte nel corso di questo incontro, e precisamente al come gestire la privacy dell'utente e del cittadino informatico. Su questo aspetto l'A.I.I.P., appunto nelle sedi internazionali, ha redatto in bozza alcune proposte di autoregolamentazione, che prendono l'avvio proprio da quanto il dottor Buttarelli sollecitava, e che riteniamo debbano essere coordinate in sede internazionale,

Alla base del sistema deve esservi l'informazione all'utente, lo sviluppo della cultura, l'alfabetizzazione, per far sì che l'utente sappia che cosa succede dei suoi dati. Una delle proposte contenute nella nostra bozza prevede di "informare gli abbonati delle modalità di fruizione dei servizi, dell'eventuale insicurezza di determinati servizi, del trattamento dei dati personali e delle possibilità di accesso ai contenuti critici".

Questo, in fondo, è un principio scontato, ed è correntemente osservato - ad esempio - anche da tutti i provider negli Stati Uniti. Quella che comincia a diventare più delicata è l'area relativa all'identità degli abbonati, quando si passa dal diritto all'anonimato, che è naturale sulla rete, al concetto di anonimato protetto, per essere sicuri di poter rintracciare il nostro utente, qualora se ne presenti la necessità. Questo aspetto non è poi tanto semplice da affrontare, anche a livello competitivo. Negli Stati Uniti esistono per esempio servizi come hot mail, dei quali un italiano può tranquillamente fruire: della propria casella di posta elettronica si può fare ciò che si vuole, protetti dall' anonimato.

Come provider, noi in Italia siamo in grado di impegnarci a garantire l'anonimato protetto, utilizzando le tecnologie che stanno emergendo. Infatti, la fotocopia della carta di identità, richiesta all' utente quando si abbona, e che è stata qui citata come un elemento purtroppo facilmente falsificabile, non rappresenta la soluzione. Dovremo quindi avvalerci degli sviluppi della firma e del certificato digitale, e siamo disponibili ad approfondire le modalità di utilizzo di questi strumenti per garantire che si possa sempre identificare, se necessario, l' autore di qualsiasi azione sulla rete. Va però detto che si tratta di un problema che non si può limitare a questa sede, ma che deve essere inquadrato a livello sovranazionale, perché altrimenti sarebbe sufficiente per un criminale rivolgersi ad un servizio all' estero per praticare azioni illecite anche sui cittadini italiani utenti della rete.

A proposito dell'ultimo punto di cui abbiamo accennato in precedenza, cioè quello relativo ai contenuti sensibili e potenzialmente critici, possiamo invece orientarci verso l'utilizzo di nuove tecnologie che consentono l'utilizzo da parte dell' utente di appositi filtri che prevengano l'accesso a contenuti dannosi. Anche in relazione a questo aspetto noi siamo disponibili a fare in modo che l'utente possa accedere per esempio ai browser che possano filtrare i contenuti, e possiamo anche considerare che sia possibile operare direttamente alla fonte una classificazione dei contenuti che ne permetta la successiva riconoscibilità, ma ancora una volta occorre essere attenti a non cadere nelle trappole tese da coloro che propongono le troppo facili soluzioni.

E qui va considerato il rischio, giustamente osservato dal professor Rodotà, che quando si cominciano a classificare i contenuti si incorre nell' inevitabile tranello della censura. Per non contare che il rischio maggiore è di essere totalmente inefficaci: quando i contenuti sono estremamente numerosi e le azioni degli utenti le più diverse, la censura comunque

sarebbe utilizzata in una percentuale molto bassa. Va considerato quindi che anche se l'Unione Europea ha in effetti deciso di stanziare grossi fondi per sperimentare i filtri elettronici, questa azione va a nostro parere considerata ancora a livello di sperimentazione.

Per concludere, desidero ringraziare ancora dell'invito, e dare tutta la disponibilità della nostra Associazione, per far sì che quella che è ancora una bozza di autoregolamentazione di settore, con tutti i suoi limiti, possa diventare al più presto un completo codice di deontologia. Proponiamo - come del resto abbiamo fatto in altra sede, ad esempio presso il Ministero delle Telecomunicazioni in tema di tariffe - di aprire un tavolo di confronto a tutti gli operatori interessati, affinché si confrontino ed arrivino nel più breve tempo possibile ad una autoregolamentazione che sia adeguata all'alto riconoscimento che questa Autorità ha in Italia ed in Europa.

Cons. Giovanni Buttarelli

Ringrazio a nome di tutti i presenti il dottor Barbuti. Il suo intervento è stato più che opportuno ed in particolare ha richiamato l'attenzione sul fatto che quando parliamo di diritti e di responsabilità, spesso ci riferiamo solo ai diritti degli utenti ed alle responsabilità dei *provider*.

Sarebbe invece opportuno - ed è un peccato che non si abbia ora il tempo per farlo - spostare l'attenzione sulle pari opportunità dei *provider* e, ad esempio, valutare se determinati diritti di segreteria, che si prefigurano nell'ambito delle procedure di autorizzazione, siano o meno produttivi di effetti nella rete.

Abbiamo un calendario molto stretto e dobbiamo purtroppo mutare l'ordine dei lavori, per permettere un'apertura tempestiva della successiva sessione e, di seguito, il collegamento in videoconferenza con Bruxelles, per l'intervento del Commissario Monti. Quindi ci permettiamo, per ora, di chiedere un piccolo sacrificio per tre richieste di intervento.

La prima richiesta riguarda la dottoressa Margot Frölinger, che non ha potuto raggiungerci ieri e che avrebbe dovuto fare una comunicazione sul commercio elettronico.

Il secondo intervento previsto è dell'avvocato Ancora, che rappresenta uno dei fornitori italiani della telefonia mobile, il quale intende affrontare il delicato problema della finalità e della conservazione nel tempo dei dati relativi al traffico. Si tratta di uno degli aspetti importanti che, come sapete, riguarda anche Internet e che è affrontato dalla direttiva cosiddetta ISDN, a cui ieri abbiamo fatto frequentemente cenno.

Infine, il terzo intervento è del dottor Catania, che rappresenta l'Associazione naziona-

le dei fornitori di video-audio informazioni. Ritengo che egli voglia parlarci delle esperienze in materia di codici deontologici, che si affiancano a quelle già menzionate.

Chiediamo cortesemente a queste tre persone, ed agli altri che dovessero chiedere di intervenire, per ora un piccolo sacrificio, a puro titolo cautelativo, per essere in grado, dopo questa pausa che speriamo di poter condensare in 15 minuti, di riaprire tempestivamente la sessione che riguarda l'importante tema dell'autoregolamentazione e che sarà presieduta dal professor De Siervo. Potremo così essere in grado, alle 11, di aprire puntualmente la video-conferenza con Bruxelles.

Vi chiediamo pertanto di contenere questa prima pausa nello spazio di 15 minuti. Grazie.

V SESSIONE

Prof. Ugo De Siervo
Componente, Garante per la protezione dei dati personali

Diamo inizio alla quinta ed ultima sessione di questo intenso convegno, con una mia brevissima introduzione. Successivamente, come avrò modo di dire, ascolteremo alcuni autorevolissimi interventi, cui seguirà la relazione del settore.

Io credo che quanto abbiamo ascoltato in questi giorni abbia indotto tutti a riflettere sulla urgente necessità di regole, a tutela di volta in volta della sicurezza delle reti e della riservatezza personale di coloro che sono oggetto delle comunicazioni e degli stessi utilizzatori di Internet. Occorrono regole a protezione degli interessi delle diverse parti coinvolte nelle comunicazioni e nel commercio elettronico, e regole a garanzia dell'effettività delle responsabilità connesse ai contenuti delle comunicazioni trasmesse.

Ma se comune è l'esigenza, diverse sono le concrete soluzioni che si possono ipotizzare, sia per le scelte differenziate sul piano dell'opportunità, sia per la diversa natura dello strumentario giuridico normalmente utilizzato nei diversi Paesi. Credo che nessuno possa realisticamente ipotizzare che fenomeni del genere di quelli cui ho appena accennato possano trovare una regolamentazione solo tramite strumenti normativi di natura pubblicistica, o invece esclusivamente di natura privatistica.

Peraltro, come abbiamo anche sentito ieri, i modelli praticati, o che vengono progettati appaiono ancora alquanto diversi da Paese a Paese, con anche una evidente, manifesta differenziazione di orientamento tra i Paesi dell'Unione europea e gli Stati Uniti d'America. Ma a ben vedere, in qualche misura entrambi questi diversi approcci generali debbono fare i conti con le tipiche caratteristiche di uno strumento particolarissimo di comunicazione, quale è Internet.

Queste caratteristiche anzitutto riducono la speranza che una disciplina esclusivamente legislativa possa essere davvero idonea o sufficiente, ma dall'altra, la grande consistenza degli interessi in gioco, la notevole delicatezza di tanti profili personali posti a rischio da possibili cattivi usi di questo strumento, rendono palese l'insufficienza dei soli strumenti di autodisciplina posti in essere dalle categorie, o dai soggetti più direttamente interessati.

Il vero problema è, quindi, la formazione di efficaci *cocktails* di fonti, quali pubbliche, quali categoriali, quali tecniche, quali contrattuali; ma c'è di più, poiché il problema poi

deve essere probabilmente trattato in modo diversificato, a seconda del tipo di dati personali trattati tramite Internet.

Solo per accennare a due tra i molti settori che utilizzano Internet, basti pensare ai ben diversi problemi posti dal commercio elettronico, o invece dalla telemedicina che usi Internet. E poi sappiamo bene che è impreciso parlare genericamente di fonti statali, o invece di autodisciplina, perché ben difficilmente si possono ipotizzare in questa materia fonti statali minuziosamente analitiche, mentre dall'altra parte viene solo raramente proposta un'autodisciplina integralmente libera.

Si pensa piuttosto, anche su questo versante, a forme più o meno obbligatorie di autodisciplina, o a forme di autodisciplina sottoposte a qualche tipo di controllo pubblico. E qui noi ne abbiamo alcuni esempi nella stessa legge n. 675 del 1996.

Si consideri, inoltre, che nei Paesi che non hanno ancora adottato una specifica, ed auspicabile, puntuale normativa su Internet, ma che hanno già recepito la direttiva dell'Unione europea n. 46 del '95, si applicano fin da ora a Internet le norme di principio contenute nella legge di recepimento, con la conseguenza che dall'entrata in vigore di queste leggi, gli operatori e gli utenti di Internet non hanno più quella sorta di extra territorialità di cui, un po' confusamente in verità, si è da qualcuno parlato.

Ma vorrei aggiungere che anche prima di tutto ciò, vigenti sono le disposizioni costituzionali coinvolte da questa nuova forma di comunicazione. Credo di non essere troppo deformato dal mio mestiere - io sono professore di diritto costituzionale - quando dico che in Italia, anche prima di ogni legislazione ordinaria, una fondamentale bussola giuridica nel trattamento di Internet ci è fornita dalla Costituzione della Repubblica, ove si considerino le sue premesse personalistiche, le sue ampie libertà civili e politiche, le sue articolate disposizioni in materia di libertà economiche ed in materia di assetto sociale.

Ma l'esistenza di una rete di princìpi costituzionali generali, ed anche la presenza di alcune disposizioni legislative contenute nella legge n. 675, ma non specifiche allo strumento Internet, espongono ad alcuni pericoli, poiché diviene eccessiva la discrezionalità di chi deve far rispettare, o in via amministrativa, o in via giurisdizionale, le generiche o incomplete disposizioni di cui disponiamo.

Tra l'altro, proprio negli ultimi mesi si sono manifestati alcuni esempi un po' preoccupanti delle conseguenze di questa incertezza, o del parziale vuoto normativo. Mi riferisco, in estrema sintesi, alle prime sentenze giurisdizionali in materia di Internet, alquanto dubbie o che sembrano navigare un po' troppo liberamente tra pochi punti sicuri. Mi riferisco pure ad alcune tendenze alquanto pericolose, a mio personale parere, di controlli generalizzati da parte di organi di indagine della magistratura, a volte di alcuni corpi di polizia, di alcune tendenze a controlli eccessivamente generalizzati sui dati di cui dispongono alcuni *providers*.

Si è fatto prima riferimento a qualche rischio che potrebbe derivare da una legislazione un po' episodica, un po' casuale, che preveda sanzioni penali particolari per problemi del tutto rispettabili a carico dei *providers*, o di altri soggetti che usino a fini penalmente riprovevoli lo strumento. Da ciò l'urgenza di arrivare ad una normazione specifica ma generale sullo strumento Internet, utilizzandosi le diverse fonti disponibili.

In Italia noi abbiamo, al momento attuale, una delega legislativa prevista nella legge n. 676, ma certo il dubbio di fondo, già esplicitato nella relazione introduttiva, è che una legislazione davvero adeguata sullo strumento Internet possa essere effettivamente adottata entro il prossimo luglio, o se non occorra invece un limitato, puntuale rinnovo della delega, in modo anche da coordinare questa legislazione con i complessi confronti, molto avanzati, che a livello di Unione europea, stanno progredendo.

Comunque, non spetta certo a me entrare nel merito della materia. Sentiremo tra poco sul tema uno dei massimi esperti della disciplina sulla tutela della riservatezza, il professor Spiros Simitis, notissimo docente di diritto privato all'Università di Francoforte, già Garante alla *privacy* per un lunghissimo periodo nel *Land* tedesco dell'Assia.

Ma prima ancora della relazione del professor Simitis, siamo molto lieti di ascoltare in teleconferenza l'intervento del professor Mario Monti, Commissario dell'Unione europea per i problemi del mercato interno e della fiscalità, e successivamente avremo l'ulteriore piacere di sentire le parole del Ministro di grazia e giustizia, professor Flick, che ha seguito con grande attenzione, e segue tuttora, la legislazione italiana sulla riservatezza.

Professor Monti le diamo il benvenuto e attendiamo la sua parola.

Prof. Mario Monti

Commissario dell'Unione Europea con i problemi del mercato interno e della fiscalità

Buongiorno. Ringrazio il Presidente, professor Rodotà per l'invito a questo convegno; purtroppo impegni sopravvenuti mi hanno trattenuto a Bruxelles.

Desidero prima di tutto cogliere l'occasione per rendere omaggio all'attività svolta dal Garante per la protezione dei dati personali, ad un anno di distanza dall'entrata in vigore della legge n. 675.

La prima relazione annuale del Garante, presentata pochi giorni or sono alle Camere, sembra confermare quanto tale normativa rispondesse non solo a criteri basilari di civiltà giuridica, ma anche ad un reale bisogno di tutela. Ho letto che in questi pochi ma intensi mesi di attività, il Garante ha già ricevuto 25 mila richieste di informazione, 250 mila notificazioni ed oltre novemila richieste di autorizzazione al trattamento dei dati censiti.

Al di là dell'aspetto quantitativo, mi sembra poi giusto sottolineare come l'impegno personale ed il prestigio del Presidente e dei membri prescelti per questo incarico, abbiano già fatto del Garante un punto di riferimento ascoltato e rispettato, in una materia che in Italia era stata a lungo e, se permettete, inspiegabilmente trascurata sul piano legislativo.

Oltre all'attività svolta sul piano nazionale, voglio sottolineare con gratitudine il contributo del Garante all'elaborazione degli orientamenti comunitari nell'ambito del gruppo dei Garanti, istituito dalla direttiva n. 95/46, gruppo del quale il professor Rodotà ha recentemente assunto la Vice Presidenza, a conferma del prestigio di cui gode sul piano internazionale.

Alle doverose congratulazioni per quanto già realizzato, vorrei tuttavia affiancare un auspicio rivolto al futuro e collegato alle mie responsabilità istituzionali di Commissario. Mi riferisco al recepimento della direttiva n. 95/46 nell'ordinamento italiano, recepimento di cui la legge n. 675 costituisce solo una parziale anticipazione, ma rispetto al quale alcuni elementi essenziali fanno tuttora difetto, e questo a pochissimi mesi dalla scadenza prevista in sede comunitaria.

Senza entrare ora ed in questa sede nel merito delle questioni giuridiche che andranno risolte di qui al 24 ottobre - questa è la data - mi preme tuttavia ricordare che la direttiva persegue due obiettivi indissociabili: da un lato si tratta della protezione dei dati personali e, dall'altro, della libera circolazione di tali dati all'interno dell'Unione europea.

Se è vero che il primo di questi obiettivi costituisce il presupposto logico del secondo, è anche vero che il coronamento di quest'ultimo, e cioè la libera circolazione, rappresenta un passaggio ineludibile ai fini del corretto recepimento della direttiva.

Il mio auspicio è che nelle prossime settimane, e nell'ambito della delega ricevuta dal Parlamento a questo fine, il Governo italiano possa completare il quadro normativo nazio-

nale, nei modi e nei tempi imposti dagli obblighi comunitari, che derivano dalla direttiva n. 95/46. Per quanto mi riguarda, assicuro che i miei servizi alla Commissione saranno come sempre a completa disposizione delle autorità italiane, per sciogliere eventuali dubbi e assicurare la corretta articolazione della normativa nazionale rispetto al disposto comunitario.

Vengo ora più vicino all'oggetto specifico di questo convegno: le regole a tutela della riservatezza nelle reti telematiche. Nonostante l'inflazione di incontri e convegni dedicati ad Internet in generale, trovo la scelta degli organizzatori particolarmente felice, per due principali ragioni, ed in primo luogo perché le reti telematiche rappresentano un serio banco di prova per la tutela effettiva della riservatezza. Mi riferisco alla perseguibilità, in concreto, dei comportamenti illeciti.

La caratteristica di Internet è quella di trascendere le frontiere geografiche e abbattere quelle temporali, in misura tale da far ritenere che nel lasso di tempo necessario per redigere un atto di citazione o un avviso di garanzia, l'attività illecita sarà già stata delocalizzata in direzione dei cieli più clementi. Questo è, d'altronde, uno degli argomenti che militano in favore di un'autorità di controllo indipendente e garante del rispetto della normativa esistente, la cui funzione è anche quella di assistere i cittadini smarriti nel labirinto del diritto internazionale privato e delle convenzioni internazionali.

Su questo aspetto, credo di poter dire che il modello europeo ha dimostrato tutta la sua validità. So bene che in altri ordinamenti giuridici la tutela della riservatezza è rimessa esclusivamente alla capacità di reazione, in forma di richieste risarcitorie, del singolo individuo, ma non posso esimermi dal pensare che in questo tipo di soluzione sono insiti due rischi opposti, ma ugualmente rilevanti: quello di una eccessiva giudizializzazione delle controversie, con l'onerosità che questa comporta per tutte le parti interessate, ed al tempo stesso il rischio che la soluzione si riveli illusoria per il cittadino normale, in ragione del costo e dei tempi oggettivamente dissuasivi della giustizia ordinaria.

In secondo luogo, se Internet è un banco di prova per la tutela della riservatezza, quest'ultima rappresenta a sua volta la precondizione per lo sviluppo di quello che viene comunemente definito come commercio elettronico. Tutte le ricerche di mercato ed i sondaggi realizzati negli ultimi anni, concordano infatti su un punto: l'importanza che gli utenti attuali e potenziali delle reti telematiche annettono alla protezione dei dati personali.

Questi sondaggi mostrano che la protezione dei dati personali, che qualcuno potrebbe vedere come un ostacolo allo sviluppo del commercio elettronico, in realtà al contrario ne rappresenta il presupposto necessario dal punto di vista degli utenti. Come ogni forma di commercio, anche questa suppone, infatti, l'incontro di una offerta e di una domanda e le preoccupazioni espresse sul versante della domanda rappresentano un passaggio che non si può eludere, se si vuole garantire al commercio elettronico un decollo reale e duraturo.

Queste esigenze sono, in effetti, alla base delle ragioni che hanno portato all'adozione della direttiva n. 95/46, difese dalla Commissione in tutte le sedi internazionali attualmente impegnate nella definizione di regole e di princìpi applicabili al commercio elettronico.

Vorrei citare, senza la pretesa di essere esaustivo, in primo luogo l'Organizzazione mondiale del commercio, nel contesto della quale la Commissione propone di avviare una

discussione finalizzata alla definizione di alcuni princìpi vincolanti su scala globale. Inoltre, l'Organizzazione per la cooperazione e lo sviluppo economico ha deciso di riservare alla *privacy* un posto di rilievo nell'ordine del giorno del prossimo vertice di Ottawa, al quale sarò presente con i miei colleghi Commissari Brittan e Bangeman. Ed anche il Consiglio d'Europa, nel cui ambito la Commissione ha coordinato con successo la posizione degli Stati membri, al fine dell'elaborazione delle linee guida per la protezione della riservatezza su Internet.

Vorrei fare una osservazione circa una dimensione internazionale della direttiva europea sulla protezione dei dati personali, che forse non è, questa dimensione, sempre presente nel dibattito. Ebbene, è proprio la direttiva europea sulla protezione dei dati personali che dal prossimo ottobre consentirà all'Unione europea di impedire il flusso di dati personali verso quei Paesi terzi che non garantiscano un livello adeguato di protezione della riservatezza.

Siccome è facile immaginare quanto grave sarebbe, per l'ordinato flusso delle informazioni e dei dati a livello globale, se ci trovassimo nelle condizioni di dover impedire il flusso, da parte europea, di dati personali a Paesi non sufficientemente garantisti da questo punto di vista, proprio per evitare questo, da tempo la Commissione preme sui *partners* internazionali, a partire dagli Stati Uniti, affinché adeguino le loro normative, o almeno le loro prassi, purché con garanzie sufficienti, per portarle, normative e prassi, a questo livello adeguato di protezione, che è tipico dell'ordinamento che ci siamo dati in Europa, proprio per evitare disturbi al flusso internazionale.

Torno sulla problematica del commercio elettronico per osservare che questa non si esaurisce certo nei soli aspetti relativi alla tutela dei dati personali. E qui, se mi è consentito, vorrei esprimere la mia soddisfazione per il fatto che questo convegno, che ho seguito a distanza - ma in questa materia la distanza conta sempre meno - ha dedicato una sessione specifica alla protezione della proprietà intellettuale. Infatti, è essenziale comprendere bene quali siano gli obiettivi dei due diversi tipi di protezione, che in tutti e due i casi riguardano diritti soggettivi: la protezione della proprietà intellettuale e la protezione dei dati personali.

Per quello che riguarda la proprietà intellettuale, già in passato la Commissione ne ha riconosciuto l'importanza vitale per la creazione di un ambiente che stimoli la creatività e gli investimenti, in modo da realizzare le condizioni perché si possano cogliere le opportunità offerte dal Mercato unico europeo.

Negli ultimi dieci anni la Commissione ha svolto un'attività particolarmente intensa, che ha portato alla definizione del quadro giuridico del diritto della proprietà intellettuale. Le cinque direttive già adottate costituiscono, a giudizio non solo nostro, un quadro giuridico solido per la protezione delle opere distribuite all'interno del Mercato unico.

Il ruolo della tutela della proprietà intellettuale è destinato ad acquisire sempre maggiore importanza nella società dell'informazione. In questo mercato in rapida evoluzione, la produzione, il valore aggiunto dei beni e servizi protetti da diritto d'autore sono cresciuti in maniera considerevole negli ultimi anni, come è noto. Ed il contesto giuridico deve garantire tale sviluppo, nel rispetto dell'equilibrio degli interessi contrapposti.

Inoltre, le nuove tecnologie hanno agevolato un ulteriore incremento dello sfrutta-

mento transfrontaliero delle opere letterarie, musicali o audiovisive e delle altre esecuzioni protette. Questa tendenza, che è senza dubbio destinata a proseguire, rende necessario garantire un effettivo mercato unico per i prodotti e servizi tutelati da tali diritti.

A livello comunitario, la Commissione ha presentato il 10 dicembre 1997 una proposta di direttiva sull'armonizzazione di alcuni aspetti del diritto di autore e dei diritti connessi nella società dell'informazione. Devo dire che la Commissione, come sua politica generale, in questa fase cerca di ridurre al minimo la produzione di nuova legislazione europea; vi sono però dei campi, dei settori, degli aspetti del Mercato unico, emergenti, che richiedono, proprio perché il settore nasca unico e non frammentato in 15 settori nazionali, la predisposizione di un adeguato quadro regolamentare. È il caso della Società dell'informazione, che ci vede molto impegnati in una attività di formazione legislativa di questo quadro, e qui in particolare l'accenno è al diritto d'autore, nella Società dell'informazione.

Questa proposta di direttiva è il risultato di un compromesso che ritengo equilibrato, tra i diritti di proprietà dei prestatori di contenuti - per esempio l'industria del software, l'industria fonografica, i produttori di film, gli editori - e dall'altra parte gli interessi perfettamente legittimi dei consumatori, degli utenti e dei prestatori di servizi on line.

Naturalmente, altre iniziative fondamentali sul piano comunitario sono necessarie per garantire la libera circolazione dei servizi in ambito Internet, ed a queste vorrei dedicare gli ultimissimi minuti di questo mio intervento.

Il commercio elettronico è destinato a beneficiare dell'esistenza del Mercato unico europeo, ed al tempo stesso contribuirà alla sua riuscita. Le dimensioni del Mercato unico vanno ben al di là della massa critica necessaria per assicurare il break even point di molti servizi elettronici e poi, a somiglianza del commercio elettronico, il Mercato unico europeo non conosce frontiere.

È un lavoro quotidiano abbattere frontiere che in forma occulta, qualche volta, si cerca di erigere; in conseguenza, il Mercato unico fornisce le fondamenta ideali, e già pronte, su cui basare un quadro regolamentare appropriato.

Nostro obiettivo è incoraggiare lo sviluppo del commercio elettronico in Europa. Esso richiede un quadro legislativo leggero, chiaro, coerente e prevedibile, che fornisca certezza giuridica alle imprese ed ai consumatori, protezione adeguata degli obiettivi di interesse generale e promozione di un ambiente competitivo.

Non è tanto necessario imporre nuove regole, quanto chiarire e adattare le regole esistenti, al fine di rimuovere le barriere legali e l'incertezza giuridica, e promuovere lo sviluppo del commercio elettronico. Questo approccio, che consiste nella rimozione delle barriere, deve essere sottolineato. I servizi della Commissione stanno esaminando un certo numero di questioni che sono fonte di incertezza giuridica, o di barriere regolamentari derivanti dalla divergenza delle legislazioni nazionali. Tali questioni stanno frenando lo sviluppo del commercio elettronico ed è mia intenzione affrontarle in una proposta di direttiva, in corso di preparazione.

La direttiva chiarirà alcune nozioni giuridiche a livello comunitario e si tratta di questioni che riguardano, tra l'altro, la definizione del luogo di stabilimento dei fornitori di

servizi della società dell'informazione; il diritto contrattuale come, ad esempio, il riconoscimento dei contratti elettronici; le comunicazioni commerciali, nel senso se debba o meno considerarsi pubblicità un sito commerciale sulla rete; la responsabilità dei fornitori di accesso e di servizi Internet.

Viene anche affrontata la delicata questione della responsabilità indiretta per gli atti compiuti da terzi, e alcuni aspetti delle professioni regolamentari, in particolare, la possibilità di fornire alcuni servizi in linea.

In conclusione, un'ultima riflessione mi sembra importante, per rispondere alla domanda posta nel titolo stesso di questo convegno: quali regole.

Non vi è dubbio che la natura globale di Internet mal si concilia con regole puramente nazionali. Quanto alle regole definite a livello comunitario, queste trovano applicazione in un'area economica che già esprime la più grossa percentuale degli scambi internazionali. Inoltre, queste regole esercitano una forza di attrazione non trascurabile nei Paesi candidati all'adesione dell'Europa centro-orientale, che ci porta ad un mercato di oltre mezzo miliardo di persone.

Certo, non si tratta ancora di regole mondiali, come quelle che sarebbero auspicabili per la società globale dell'informazione, tuttavia queste regole comuni rappresentano storicamente il primo ed unico esempio di integrazione giuridica volontaria fra Stati sovrani. La storia offre altri esempi di integrazione, ma condotti con metodi più asimmetrici e fondati sulla forza spesso fisica.

A mio modo di vedere, la globalizzazione degli scambi, simbolizzata da Internet, rende lecito sperare che l'esempio comunitario possa rappresentare un modello di riferimento per un'area geografica più vasta. Infine, l'esistenza di regole comuni rafforza enormemente la capacità negoziale dei Paesi europei in sede internazionale, e questo non mi sembra proprio un aspetto trascurabile.

L'ultima battuta, signor Presidente. Oggi è la Giornata dell'Europa; si discute in questo convegno tutta una serie di problemi che sono legati, tra l'altro, alla tutela della privacy, che viene così autorevolmente asserita e condotta in Italia dal Garante. Spesso i cittadini, anche in Italia, pensano all'Europa come a qualche cosa di lontano, a qualche cosa che in questa fase storica porta ai cittadini dei singoli Stati membri dei pesi, degli oneri, degli adempimenti, delle valutazioni.

In questo momento mi piace ricordare che l'Europa porta in realtà, ma spesso non siamo capaci come cittadini di coglierlo, come responsabili europei di spiegarlo, una valorizzazione del cittadino rispetto alla società. L'esempio della privacy mi sembra significativo. Quanti cittadini italiani sanno che la tutela della privacy, così recentemente introdotta in Italia, così estranea - diciamolo pure - alla tradizione della cultura italiana, è il risultato di una direttiva europea?

Mi piace concludere il mio intervento un po' troppo tecnico, e di questo mi scuso, con questa riflessione personale sulla nostra Europa in questa giornata che le è dedicata. Grazie per la vostra attenzione.

Prof. Stefano Rodotà

Io ringrazio particolarmente il professor Monti, non solo per le parole di apprezzamento che ha avuto per il nostro lavoro, ma proprio per le parole finali.

Egli ha richiamato l'attenzione su una sorta di valore aggiunto europeo, che i cittadini di questo Continente spero cominceranno progressivamente ad apprezzare, perché il timore di un riduzionismo europeo, di una logica dell'Europa, come dice qualcuno, tutta appiattita sui problemi monetari e finanziari, trova o comincia a trovare delle smentite eloquenti in vicende come quella di cui ci stiamo occupando.

Vorrei ringraziare il professor Monti per il suo intervento, che non è tecnico, ma centrato nel merito politico di questioni delicate, con richiami specifici a noi, con indicazioni importanti per il Governo, ed anche per due riferimenti, direttamente relativi al tema del nostro convegno.

Egli ha richiamato l'attenzione sulla necessità di un quadro istituzionale, ridefinendone però anche le caratteristiche. Ha parlato di un quadro normativo leggero, un termine che a me piace molto, che, mi permetto di dire, adopero anch'io da lungo tempo e che corrisponde alle esigenze del settore di cui ci stiamo occupando e, più in generale, della evoluzione dei nostri sistemi giuridici nelle aree così profondamente segnate dalla innovazione scientifica e tecnologica.

L'altro aspetto è legato, come ricordava il professor Monti, alla creazione di uno spazio giuridico in Europa, che può costituire un punto di riferimento per un'area geografica più vasta. L'opera che la Commissione sta svolgendo, e che il professor Monti ci ha ricordato parlando di pressione sui *partners* internazionali, perché adeguino le loro legislazioni nazionali, o i loro sistemi ai valori, ai criteri ed ai livelli di protezione adottati in Europa, è di straordinario significato, perché accanto alla circolazione transnazionale di dati, forse un po' enfaticamente mi permetterei di dire che possiamo assistere ad una circolazione transnazionale di valori.

L' Europa ha riflettuto con grande intensità sul problema della tutela della privacy.

Non vorrei usare un'espressione eccessiva, è un concetto nato negli Stati Uniti, che ha trovato condizioni di crescita particolarmente favorevoli in Europa, in questi anni, affermando un valore che è valore di cittadinanza. Ed allora l'Europa riscopre anche un'antica vocazione ad essere nel mondo portatrice di valori. Per questo riferimento, torno a dire, la nostra gratitudine al professor Monti è particolare.

Adesso restituisco la parola e la direzione di questa sessione all'amico De Siervo.

Prof. Ugo De Siervo

Ringraziamo ancora il professor Monti per le sue parole assai costruttive e stimolanti. In particolare vi è un punto che mi permetterei, ad integrazione di quello che ha detto Stefano Rodotà, di richiamare.

Il professor Monti, all'inizio del suo intervento, ha ricordato come l'Italia debba ancora dare integrale attuazione alla direttiva n. 95/46, ed uno dei punti di questa integrale attuazione concerne proprio due temi di cui ci siamo occupati in questi giorni: da una parte l'ordinamento di Internet, dall'altra il commercio internazionale tramite strumenti telematici.

Questo mi sembra uno stimolo ulteriore, che trasmetteremo sia al relatore che al Ministro Flick, non appena potrà essere tra noi. Anzi, a questo punto io mi permetterei di invitare il professor Simitis a svolgere la sua relazione, invertendo lievemente l'ordine che avevamo prima progettato.

Prof. Spiros Simitis
Goethe Universität - Frankfurt am Main

Thank You Chairman. Let me start with a very personal remark. It is certainly not the first time that I have the chance to address in Italy problems related to data protection. But it is, much to my pleasure, for sure the first time that I have not to concentrate my remarks on the necessity of mandatory rules guaranteeing an efficient protection. After so many years of long and complicated debates Italy has joined those states of the European Union that already have enacted data protection laws.

May I also remind You that the Italian law was adopted at the end of 1996, closely followed by another late-comer, Greece, in early 1998. The last were thus the first. They were the last because Italy and Greece were the only Member States of the European Union that had no legislation. But they were also the first for the reason that no other Member State transposed so quickly the Directive. Now, if one looks at these two laws one substantial difference that directly concerns our debate can be easily discerned. While the Italian law sticks with regard to the transfer of data to the Directive, the Greek law is definitely more rebellious. It simply renounces to a provision corresponding to art. 26 of the Directive and refuses thus to explicitly accept that the adequacy demand can be fulfilled by self-regulation.

However, even if both laws react differently, their approach can lastly only be correctly interpreted against the background of a general policy of the Directive that though expressly mentioned in the Recitals tends to be forgotten, or, should I say, repressed. Data protection is in the Directive's view an open process. The Directive does in other words not give definitive answers. It incites, on the contrary, the Member States to continuously try to develop new and better ways of guaranteeing an efficient protection. Only then the Member States will be able to respond to the Directive's appeal to understand and implement data protection as an essential means for securing the fundamental rights of the data subjects. And only then the Member States will have a chance to adapt the rules governing the processing to both the demands of the various contexts of processing and to the challegnes of a constantly changing technology. In short, Greece and Italy act in a different way within what the Directive calls their margin of manoeuvre.

The result is however what in these days has been described, especially in connection with the consequences of the Directive for the transfer of data to and from the United States, as a major conflict, an assumption which in the opinion of some commentators justifies the conclusion that October 24, the date by which the Directive will have to be transposed by the Member States, is the D-day of data protection. One even could go further and argue that due to the differences between the Italian and the Greek law the transatlantic confrontation has now extended to a no less severe intra-European discord.

Neither of these presumptions can be supported either by the history of data protection or by the intentions of the Directive and the actual developments in the Member States.

Let me first remind of the times when the Directive did not yet exist. International transfers may have been less intensive, they nevertheless played an important role. It is therefore not surprising that those countries that already had laws were forced to develop rules concerning the transborder flow of data. And as astonishing as it may sound the result was, despite the differences between the various laws, a common approach: the equivalence principle. Some countries, like in Scandinavia, expressly included it in their written law, others, like Germany, implemented it, both by law and through the activities of the Data Protection Commissioners.

It is because of this principle that, for instance, the Swedish Data Protection Commissioner strictly opposed a transfer of data of Swedish citizens to Great Britain in relation with the introduction of a particular health card on the grounds that Great Britain had no provisions securing a protection of the data. For exactly the same reasons the Hesse Commissioner rejected shortly after a transfer of specific health data to the Netherlands where they would have been processed in order to establish an international register on certain illnesses. The same considerations incited the Austrian Commissioner to prohibit the transfer of employee data to a country in which, contrary to Austria, there were no rules empowering the employees' representatives to participate in the employer's decisions on the uses of the employee data. Finally, the plans of General Motors to centralise the processing of employee data failed because of criticisms very much on the line of the Austrian considerations. We can therefore easily conclude that the problems we are discussing are by no means new.

Let me also stress a second equally relevant point. The more the first generation of omnibus rules was followed by regulations that deliberately complement the general principles by sectoral context-oriented provisions, the more the flexibility of the rules grew and the more it appeared possible to adjust the demands for a transfer to the specific characteristics of the intended processing. The most recent attempt to maximise flexibility is the inclusion of self-regulation first in the British and in the Dutch laws and later in the Directive. It is hence not correct to assume that self-regulation is virtually unknown to data protection laws.

However, neither the national laws nor the Directive regard self-regulation as an alternative to mandatory rules. They may openly promote self-regulation but they at the same time unequivocally clarify that it is an additional regulatory element and therefore under no condition a both satisfactory and sufficient answer to the problems arising out of the processing of personal data. In other words, as the Directive overtly states, rules developed by the controllers have in order to be accepted to go through a particular procedure. They must first and foremost comply with the demands contained in the data protection laws.

Moreover, they are only accepted as a valid regulatory instrument if they have been submitted to the supervisory authorities and to the extent that they have been approved by them.

This is why Italian and Greek law reflect, despite their different approach, a common perception of the transfer to third countries. When decisions affecting its admissibility have to be taken, they must respect the ranking that has also been affirmed by the Art. 29 Group: The adequacy presupposes first and foremost mandatory rules. They certainly must

neither be part of a comprehensive data protection law nor cover all the aspects regulated by the laws of the Member States and the Directive, or adopt in every respect exactly the views expressed by the European Union. The processing of personal data has however to be subjected to a binding regulation based on a law. Self-regulation can therefore help to detail and increase the protection of the data subjects but not displace mandatory rules. It is, to repeat it once more, an additional regulatory element and not a means that can be put on the same level as legislative requirements.

I am of course well aware of the attempts to disqualify the demand for mandatory rules by describing them as the product of an obvious cultural difference between Europeans and Americans, the first being resolute followers of a quasi omni-present intervention of the state, the latter partisans of a decidedly libertarian approach clearly putting the accent on an autonomous decision of the parties concerned. But I am nevertheless persuaded that all such assumptions deeply disregard especially the experiences of the last decades. Where, for instance are the sources of European anti-trust or anti-discrimination laws to be found if not in American laws? And why did, contrary to the already mentioned example of the transfer of health data to the Netherlands, Data Protection Commissioners have no difficulties in agreeing to the transmission of certain medical data for research purposes to the United States, if not because of the existence of clear and binding processing rules in the research sector? Besides, if my memory does not fail, the United States did not particularly hesitate to enact mandatory provisions in the case of cryptography which shortly reemerged in similar regulatory policies of some of the European countries.

The insistence on cultural differences and consequently on the priority of self-regulation is hence no more than a typical self-defence mechanism. The very moment that the necessity of mandatory rules becomes clear, self-regulation is presented as a true and even better alternative in order to avoid, may it only be at the very last minute, a legislative decision. No wonder therefore that there is an astonishing coincidence of arguments irrespective of whether the reactions of the seventies and eighties in Germany and Great Britain or the actual debates in the United States are looked at. The answer has hence to be exactly the same as in the early years of data protection: What we need is, as Commissioner Monti also stated, a complex system of rules and not a regulation determined by the controllers and guided by their perception of the importance and the limits of the processing of personal data.

The refusal to reduce the rules governing the use of personal data to provisions based on a self-regulation reflects the conviction expressed in the parliamentary debates on the Hessen Data Protection Law of 1970, as well as in the remarks of the President of the French Republic at the address of the Commission that drafted the first proposals for a French law in 1974, the conclusions of the Federal German Constitutional Court in its seminal 1983 census-decision and last but not least the clear statements of the European Commission, the Council and the European Parliament explaining the need for a Directive. Data protection is throughout these documents regarded as a conditio sine qua non of the protection and the exercise of fundamental rights and therefore as a constitutive element of a democratic society.

Let me finish by a few observations on a different, nevertheless deeply related topic of our discussion: cyberspace. Internet is both an agora and a forum. It may often still be perceived as embodying free speech but it has since long transcended the frontiers to the market, or, to put it more bluntly, to the bazar. What we therefore witness is an increasing commodification of the individual. The case of John Moore, the by now famous patient of the University of California in Los Angeles who had been instantly qualified by the doctors involved in his treatment as a medical treasure and who only very late and by pure chance discovered that his blood and his cells had turned into an unending source of patents and had hence asked for a substantial part of the profit, should force us to consider once more carefully what the purpose of data protection really is.

Individuals surfing through the Internet are never alone. They inevitably leave traces that are continuously registered and consequently permit to compose and recompose ad libitum their data in order to produce the commercially most profitable profile. What we therefore more than ever cannot avoid is to discuss the impact of the growing commercialisation on data protection. Where it is reduced to a mere property right its original and up to now sole justification is abandoned. The only relevant question is how to secure the individual's chances to get the best possible price for her or his data. As necessary hence as a complex and at the same time flexible system of rules, as advocated by Mr. Buttarelli, is we must first be clear about the aims of the regulation.

Besides, we have in the past over and again realised the limits of a purely normative approach. Its deficiencies were already illustrated by the decentralisation of the processing achieved with the help of personal computers and by the growing use of "intelligent cards".

They are better than ever before demonstrated by the Internet. Data protection has lastly only a chance if a privacy-enhancing technology is deliberately promoted by the legislator and incorporated into both the soft- and the hardware. A globalised communication necessitates moreover an equally universalised regulatory approach. But let me repeat:

Technological changes as important as they are do not dispense from the application of those principles that guarantee the respect and the implementation of fundamental rights if the change of technology is not to change the structure of society.

Thank You.

Prof. Spiros Simitis
Goethe Universität - Frankfurt am Main

Grazie, signor Presidente. Vorrei iniziare con un'affermazione molto personale. Non è certo la prima volta che ho occasione di parlare in Italia di problemi legati alla protezione dei dati. Ma è senz'altro la prima volta che, con mio grande piacere, non devo focalizzare le mie osservazioni sulla necessità di norme vincolanti che garantiscano una protezione efficace. Dopo tanti anni di lunghe e complesse discussioni, l'Italia si è unita al gruppo degli Stati dell'Unione Europea che hanno già approvato leggi in materia di protezione dati.

Vorrei anche ricordare che la legge italiana è stata adottata alla fine del 1996, ed è stata seguita a ruota da un altro ritardatario, la Grecia, all'inizio del 1998. Gli ultimi sono dunque stati i primi. Gli ultimi, perché Italia e Grecia erano gli unici Stati membri dell'UE ancora privi di una legge in materia; sono però stati anche i primi, perché nessun altro Stato membro ha recepito la Direttiva con pari rapidità. Ebbene, se si esaminano i due testi di legge è facile individuare una differenza sostanziale che attiene direttamente alla nostra discussione. Mentre la legge italiana, quando si parla di trasferimento di dati, si uniforma alla Direttiva, la legge greca è decisamente più ribelle. Di fatto, essa rinuncia ad inserire una disposizione corrispondente all'art. 26 della Direttiva, e quindi rifiuta di accettare in modo esplicito la possibilità che il requisito dell'adeguatezza sia soddisfatto attraverso l'autodisciplina.

Tuttavia, anche se le due leggi scelgono un approccio diverso, esse possono essere interpretate correttamente, in ultima analisi, solo nel contesto di una scelta di politica generale compiuta dalla Direttiva che, per quanto menzionata esplicitamente nel preambolo, tende ad essere dimenticata - o, meglio, repressa. Il punto di vista assunto dalla Direttiva è che la protezione dei dati rappresenta un processo aperto. La Direttiva, in altre parole, non fornisce risposte definitive. Semmai, essa invita gli Stati membri ad adoperarsi costantemente per mettere a punto strumenti innovativi e migliori in grado di garantire una protezione efficiente. Solo in tal modo gli Stati membri potranno adempiere all'esortazione della Direttiva di considerare ed attuare la protezione dei dati in quanto strumento essenziale per garantire i diritti fondamentali degli interessati.

E solo in tal modo gli Stati membri avranno la possibilità di adattare le norme relative al trattamento alle esigenze dei vari ambiti di trattamento e alle sfide poste da una tecnologia in continua evoluzione. In breve, Grecia ed Italia adottano un approccio diverso nel quadro di quello che la Direttiva chiama il "margine di manovra".

Il risultato, tuttavia, è quello che in questi giorni è stato descritto, soprattutto in rapporto alle conseguenze della Direttiva sul trasferimento di dati verso e da gli Stati Uniti, come una situazione di grave conflitto - un assunto che, a giudizio di alcuni commentatori, giustifica la conclusione che il 24 ottobre, la data entro cui gli Stati membri devono recepire la Direttiva, sarà il D-day della protezione dati. Si potrebbe anche andare oltre, afferman-

do che, a causa delle discrepanze fra la legge italiana e quella greca, il confronto transatlantico si è ormai esteso all'Europa dando luogo ad un conflitto intraeuropeo di non minore gravità. Nessuna delle due ipotesi è corroborata dalla storia della protezione dati o dalle intenzioni della Direttiva e dagli sviluppi effettivamente intervenuti negli Stati membri.

Permettetemi di ricordarvi come stavano le cose quando la Direttiva non esisteva ancora. I trasferimenti internazionali di dati potevano essere meno frequenti, ma giocavano comunque un ruolo non trascurabile. Quindi, non soprende il fatto che i paesi ove già sussistevano leggi in materia abbiano dovuto definire norme applicabili ai flussi di dati transfrontalieri. E per quanto possa sembrare sorprendente, il risultato fu che, nonostante le differenze fra le singole leggi, si giunse ad un approccio comune: il principio di equivalenza. Alcuni paesi, come quelli scandinavi, le ricompresero espressamente nella legislazione positiva; altri, come la Germania, vi dettero attuazione attraverso norme di legge e con l'attività delle Autorità di protezione dati.

E' in rapporto a tale principio che, ad esempio, l'Autorità svedese di protezione dati si oppose rigidamente al trasferimento di dati di cittadini svedesi verso il territorio britannico in relazione ad una particolare tessera sanitaria che si intendeva introdurre in tale Paese, motivando tale rifiuto con l'assenza in Gran Bretagna di disposizioni che garantissero la protezione dei dati. Per lo stesso motivo l'Autorità dell'Assia respinse la richiesta di un trasferimento di specifici dati sanitari verso i Paesi Bassi, dove i dati sarebbero stati sottoposti a trattamento per creare un registro internazionale relativo a determinate patologie. Le stesse considerazioni spinsero l'Autorità austriaca a vietare il trasferimento di dati relativi a dipendenti verso un altro paese in cui, a differenza dell'Austria, non esistevano norme che consentivano a rappresentanti dei lavoratori di compartecipare alle decisioni dei datori di lavoro in merito all'utilizzo dei dati che li riguardavano. Infine, il progetto della General Motors di centralizzare il trattamento dei dati dei dipendenti fallì per una serie di critiche sostanzialmente analoghe a quelle mosse dall'autorità austriaca. Si può dunque concludere senza alcun dubbio che i problemi di cui stiamo discutendo sono tutt'altro che nuovi.

Vorrei sottolineare anche un secondo punto di pari importanza. Man mano che alla prima generazione di norme omnibus facevano seguito regole che integravano volutamente i principi generali attraverso disposizioni settoriali contestualizzate, nella stessa misura aumentava la flessibilità delle norme e sempre più appariva possibile adattare le richieste di trasferimento alle specifiche caratteristiche del trattamento previsto. Il tentativo più recente di massimizzare tale flessibilità è rappresentato dall'inclusione dell'autodisciplina prima nella legge britannica e in quella olandese, e successivamente nella stessa Direttiva. Dunque, non è corretto supporre che l'autoregolamentazione sia virtualmente sconosciuta alla legislazione in materia di protezione dati.

Tuttavia, né le leggi nazionali né la Direttiva considerano l'autodisciplina un'alternativa all'introduzione di norme vincolanti. Possono favorire esplicitamente l'adozione di codici di autodisciplina, ma al contempo affermano con estrema chiarezza che si tratta di un ulteriore elemento normativo - e dunque non rappresenta una risposta soddisfacente e sufficiente ai problemi derivanti dal trattamento di dati personali. In altri termini, come affer-

mato chiaramente dalla Direttiva, le norme elaborate dai titolari devono essere oggetto di una specifica procedura per essere accettate. In primo luogo, esse devono uniformarsi ai requisiti fissati nella legislazione in materia di protezione dati. Inoltre, sono considerate uno strumento normativo valido solo se sono state sottoposte all'esame delle autorità di controllo e nella misura in cui queste ultime vi abbiano dato approvazione.

È per tale motivo che, nonostante la diversità degli approcci adottati, la legge italiana e quella greca riflettono una percezione comune del trasferimento di dati verso paesi terzi.

Ogniqualvolta si debba decidere sull'ammissibilità di tale trasferimento, occorre rispettare l'ordine sancito anche dal Gruppo costituito ai sensi dell'art. 29: l'adeguatezza presuppone in primo luogo la presenza di norme vincolanti. Queste ultime non devono indubbiamente far parte di una legge generale sulla protezione dei dati né devono coprire tutti gli aspetti regolamentati dalla legislazione degli Stati membri e dalla Direttiva, né fare proprie in tutto e per tutto le posizioni dell'Unione Europea. Tuttavia, il trattamento di dati personali deve essere soggetto a norme vincolanti basate su un testo legislativo. L'autodisciplina può dunque contribuire a particolareggiare e potenziare la protezione degli interessati, ma non può prendere il posto di norme vincolanti. Ancora una volta, si tratta di un elemento di regolamentazione aggiuntivo, e non di uno strumento da mettere sullo stesso piano delle prescrizioni di legge.

So bene che da più parti si tenta di dequalificare la richiesta di norme vincolanti descrivendole come il prodotto di una netta differenza culturale fra europei ed americani - per cui i primi sarebbero convinti seguaci di un intervento statale pressoché onnipervasivo, mentre i secondi sarebbero a favore di un approccio decisamente libertario che pone l'accento sull'autonomia decisionale dei soggetti interessati. Sono però convinto che tutte queste supposizioni non tengono assolutamente conto soprattutto delle esperienze maturate negli ultimi decenni. Per esempio, dove si trovano le fonti della legislazione europea in materia di antitrust o pari opportunità se non nella legislazione americana? E perché, contrariamente all'esempio prima menzionato in cui si prevedeva il trasferimento di dati sanitari verso i Paesi Bassi, le autorità di protezione dati non hanno alcuna difficoltà a consentire la trasmissione negli USA di determinati dati sanitari per scopi di ricerca, se non perché esistono norme precise e vincolanti per il trattamento di dati personali nel settore della ricerca? Inoltre, se la memoria non m'inganna, gli USA non hanno avuto particolari esitazioni ad emanare disposizioni vincolanti nel caso della crittografia, disposizioni che hanno fatto la propria comparsa anche in norme analoghe emanate successivamente da alcuni paesi europei.

L'insistenza sulle differenze culturali e, quindi, sulla priorità dell'autoregolamentazione non rappresenta altro, dunque, che un tipico meccanismo di autodifesa. Nel momento stesso in cui si manifesta la necessità di norme vincolanti, viene presentata quale alternativa reale e persino migliore l'autoregolamentazione - e questo per evitare, sia pure all'ultimo minuto, una decisione di natura legislativa. Non stupisce pertanto che esista una impressionante concordanza fra le argomentazioni utilizzate, sia che si considerino le reazioni suscitate in Germania e Gran Bretagna negli anni '70 e '80 o il dibattito attualmente in corso

negli USA. La risposta non può dunque che essere identica a quella fornita quando la protezione dei dati muoveva i primi passi: quello che ci serve, per usare un'espressione fatta propria anche dal Commissario Monti, è un sistema complesso di norme e non una regolamentazione definita dai titolari e basata sulla loro valutazione dell'importanza e dei limiti del trattamento di dati personali.

Il rifiuto di ridurre le norme sull'utilizzo di dati personali a disposizioni fondate sull'autoregolamentazione riflette la convinzione espressa durante il dibattito parlamentare relativo alla Legge sulla protezione dei dati del Land Assia (1970), ed anche le considerazioni del Presidente della Repubblica francese nel suo discorso alla Commissione incaricata di redigere la prima proposta di legge francese nel 1974, le conclusioni della Corte costituzionale federale tedesca nella sentenza emessa nel 1983 in materia di censimento e, non in ultimo, le nette affermazioni della Commissione europea, del Consiglio e del Parlamento europeo in merito all'esigenza di una Direttiva. La protezione dei dati viene considerata, in tutti i documenti citati, una conditio *sine qua non* per la tutela e l'esercizio di diritti fondamentali, e quindi un elemento costitutivo delle società democratiche.

Vorrei concludere con alcune osservazioni su un tema diverso ma comunque profondamente legato alla nostra discussione: il ciberspazio. Internet rappresenta sia la piazza di un mercato che il foro. Spesso viene ancora vista come una personificazione della libertà di espressione, ma da lungo tempo ha trasceso questi limiti in direzione del mercato o, se vogliamo essere più espliciti, del bazar. Quello a cui stiamo dunque assistendo è la crescente trasformazione del singolo in un bene di consumo. Se pensiamo al caso di John Moore, l'ormai famoso paziente della University of California a Los Angeles che era stato immediatamente giudicato un vero e proprio tesoro per la medicina dai sanitari che lo avevano avuto in cura, e che solo dopo molto tempo e per puro caso scoprì che il suo sangue e le sue cellule erano divenuti una fonte inesauribile di brevetti, cosicché chiese di ricevere una porzione sostanziosa dei profitti, dovrebbe farci riconsiderare con attenzione quelli che sono gli scopi effettivi della protezione dati.

Il singolo che naviga per Internet non è mai solo. Egli lascia inevitabilmente tracce che vengono continuamente registrate e consentono quindi di comporre e ricomporre a piacere i dati che lo riguardano fino ad ottenere il profilo più vantaggioso in termini commerciali. Pertanto, quello che ora più che mai non possiamo evitare è un dibattito sugli effetti della crescente commercializzazione in rapporto alla protezione dei dati. Se si riduce ad un semplice diritto di proprietà, la sua giustificazione originaria, e finora la sola valida, viene a perdersi. L'unico quesito pertinente riguarda come garantire al singolo la possibilità di ottenere il prezzo migliore per i propri dati. Dunque, per quanto sia necessario un sistema di norme complesso e al contempo flessibile, come sostenuto dal Dr. Buttarelli, occorre che prima si faccia chiarezza sugli scopi di tale regolamentazione.

Inoltre, in passato più volte ci si è resi conto dei limiti di un approccio puramente nor-

mativo. Le deficienze di un approccio del genere sono state già evidenziate in rapporto alla decentralizzazione del trattamento ottenuta con l'aiuto dei personal computer ed all'utilizzo crescente delle cosiddette "carte intelligenti"; esse risaltano in misura ancora maggiore in rapporto ad Internet. In ultima analisi, l'unica possibilità per la protezione dati è costituita dalla scelta del legislatore di promuovere una tecnologia di potenziamento della privacy (PET) incorporandola sia nel software che nell'hardware. La globalizzazione delle comunicazioni impone inoltre un approccio normativo egualmente di ordine globale. Tuttavia, vorrei ribadire che i cambiamenti tecnologici, per quanto importanti, non dispensano dall'applicare quei principi che garantiscono il rispetto e la realizzazione di diritti fondamentali, se si vuole evitare che il cambiamento tecnologico comporti un cambiamento nella struttura della società.

Grazie.

Prof. Ugo De Siervo

Ringraziamo vivamente il professor Simitis, che ha mantenuto le promesse, per le quali avevamo avuto piacere di averlo tra noi.

È giunto il Ministro Flick, che invitiamo al tavolo della Presidenza. Egli è stato prima da noi descritto come uno dei padri principali di questa legislazione, uno di quei padri che non ha abbandonato il proprio figlio a se stesso, ma ha seguito con grande pazienza e intensità le fasi successive.

In fondo, la legge n. 675 è già stata integrata, se non ricordo male, ben quattro volte dal Consiglio dei Ministri, e lo sarà ancora; una delle tante preoccupazioni che in noi sorgeva era relativa non tanto alle correzioni, ma proprio al fatto che le integrazioni rappresentassero un panorama così vasto.

Noi qui stiamo lavorando semplicemente su uno o due filoni per i quali il Governo della Repubblica ha avuto la delega, e non possiamo nascondere l'esistenza di qualche preoccupazione relativa al fatto se il Governo potrà davvero, entro il prossimo luglio, adempiere al grande compito di integrazione legislativa, o se, al contrario, bisognerà puntare su una prima proroga di questa legislazione.

Vorrei invitare il Ministro Flick a prendere la parola.

Prof. Avv. Giovanni Maria Flick
Ministro di grazia e giustizia

Nel ringraziarLa, Presidente, mi scuso se altri impegni (meno interessanti) mi hanno impedito, come avrei voluto, di seguire i lavori sin da ieri.

La ringrazio ancora per ciò che ha detto, anche se devo specificare che non sono uno dei padri, ma soltanto uno di coloro che con voi ha lavorato e sta lavorando per affrontare una tematica alla quale culturalmente non siamo forse ancora completamente preparati.

Certamente l'approvazione della legge sulla *privacy* ha rappresentato una delle priorità che il Governo si pose sin dal momento dell'insediamento: non soltanto perchè condizionava l'ingresso dell'Italia nell'area Schengen, ma anche - e vorrei forse dire: soprattutto - per l'alto valore di principio di cui questa legge è portatrice, atteso che sottolinea, finalmente, grazie al Presidente Rodotà - lui sì che è uno dei padri di questo cammino - il passaggio da una tutela di tipo formale ad una tutela di tipo sostanziale della *privacy*.

Tale tipo di tutela trova il suo momento qualificante nella centralità del consenso dell'interessato e quindi nella possibilità, per questo, di interagire con il sistema (chiedendo la correzione dei dati erronei), nonché nel ruolo fondamentale dell'autorità del Garante in questo cammino.

Nonostante il "ritardo" con cui è stata emanata la normativa in materia di trattamento dei dati, non vi è dubbio che il modello che essa propone non si adatta alle peculiarità ben note dell'universo-Internet, rivelando così le difficoltà che incontriamo ogni volta si debba predisporre una tutela legislativa più o meno rigida in materie dotate di un elevato tecnicismo e, per questo, in continua, velocissima evoluzione.

Una difficoltà - occorre dirlo - scontata in partenza, se è vero che, come a me sembra, siamo stati tra i primi, se non addirittura il primo Paese dell'Unione a prendere atto della necessità di modulare anche in rapporto a Internet, la disciplina della protezione dei dati (penso all'art. 1, comma 1, lettera n, l. n. 676/96).

Tuttavia, non sarebbe onesto negare che la predisposizione di questa normativa incontrerà ostacoli.

Mi riferisco ad ostacoli non certo di ordine concettuale: la riservatezza ha un tale rilievo in termini costituzionali e di diritto internazionale, che non è neanche possibile ipotizzarne una compressione in questo specifico campo, le cui vastissime potenzialità fanno di Internet una temibile forma di aggressione.

Parlo, piuttosto, di ostacoli di ordine tecnico, legati ai problemi che questa materia pone, in quanto campo privilegiato e particolarmente emblematico di scontro tra la tutela della *privacy* (i diritti) e l'*humus* di più sofisticate forme di criminalità (le responsabilità).

Le reti aperte sono una realtà certamente irrinunciabile, perché costituiscono una straordinaria piattaforma, che offre ad un costo contenuto opportunità di comunicazione

fino a pochissimo tempo fa nemmeno immaginabili: comunicazione rapida, efficiente, selettiva, che ha un'importanza innegabile in sé dal punto di vista sociale e della crescita culturale dei suoi fruitori, ma che, senza dover cadere in una dimensione soltanto efficientistica e di mercato, rileva anche come strumento di sviluppo economico e lavorativo (si pensi alle imprese virtuali ed alla possibilità di valicare le frontiere nazionali, nella prospettiva di una sempre maggiore omogeneizzazione).

Al Forum della Pubblica amministrazione, al momento della presentazione al pubblico degli strumenti che in quest'ambito sta elaborando, appunto, la Pubblica amministrazione, ed in essa l'Amministrazione della giustizia, sono rimasto colpito io stesso dal salto enorme che abbiamo fatto rispetto all'analogo appuntamento di un anno fa.

Non per niente, d'altra parte e tanto per fare un esempio, la dichiarazione conclusiva della Conferenza ministeriale di Bonn, del 6-8 luglio 1997, riconosce e incoraggia questa finalizzazione in chiave di sviluppo, sottolineando, al punto 9, che "la ricchezza e la diversità di contenuti e dei servizi permetteranno non soltanto di far fronte alle esigenze dei consumatori europei, ma in un ambiente digitale che favorisce la diversità, si dimostreranno interessanti anche per utenti di altre Regioni del mondo". Anche su questo punto vorrei tornare brevemente alla fine di questa mia rapidissima riflessione, evidenziando le opportunità del commercio elettronico e l'importanza che Internet riveste per il settore privato.

È chiaro ed evidente che più sono le possibilità insite nell'impiego di Internet, più crescono le occasioni di illecito che si può commettere attraverso il sistema e ai danni di esso.

Ed è un tema al quale, per la mia pregressa esperienza culturale, oltre che per il mio ruolo attuale, sono particolarmente sensibile.

Come è noto, la conoscenza della tecnologia Internet, se non vengono adottate idonee misure di sicurezza, agevola le possibilità di intercettare e manipolare i messaggi che viaggiano su Internet, non consentendo per questo di garantire la genuinità del documento; da ciò, il ricorso alle reti chiuse, i cui utilizzatori hanno preventivi rapporti contrattuali e di reciproca fiducia, come puntualmente evidenziato dalla Commissione CEE nella comunicazione dell'8 ottobre 1997.

Ma accanto al problema dell'intercettazione e della manipolazione dei messaggi, si pone il problema della raccolta indebita dei dati personali. È nota a tutti l'esistenza di *software* che, esplorando la rete, sono in grado di mettere insieme un numero impressionante di dati disponibili, relativi ad una determinata persona.

Proprio in relazione a questa possibilità, mi ha colpito l'esempio riportato nella relazione per il 1997 del Garante per la protezione dei dati personali, la quale richiama a sua volta un articolo giornalistico nel quale si spiega come, utilizzando le informazioni tratte dai gruppi di discussione a cui una persona ha partecipato, si può ricostruirne una biografia completa e dettagliata.

Ciò crea un'inderogabile esigenza di protezione della *privacy* in rapporto ad Internet. Anche in questo caso occorrerà, una volta di più, appellarsi ai princìpi fondamentali della materia: in particolare, i dati personali devono limitarsi allo stretto necessario ed attenere la finalità lecita per cui sono stati raccolti (art. 6, comma 1, lettera c) e art. 7 direttiva

95/46/CE; art. 9 legge n. 675/96).

Se il principio è indiscusso e indiscutibile, appare tuttavia evidente che, in assenza di forme di controllo a monte, la semplice comminatoria della sanzione penale potrebbe rivelarsi inefficace. La cifra oscura dei reati sarebbe presumibilmente assai elevata e la garanzia di immunità non rappresenta certo un deterrente a delinquere, tanto più - e mi ricollego all'intervento che ho ascoltato prima - ove si consideri la caratterizzazione economica insita nello sfruttamento di questi dati a fini commerciali.

Dunque, prima ancora che sull'individuazione delle responsabilità, il discorso si appunta sulla necessità di predisporre adeguate forme di prevenzione. Ma sarei presuntuoso se volessi soffermarmi sull'argomento, conosciuto da voi meglio che da me.

Ricorderò solamente le due ipotesi della crittografia e dell'anonimato, che possono consistere, alternativamente o congiuntamente (in considerazione della tipologia dei dati trattati e del tipo di trattamento) in regole giuridiche o in forme di autodisciplina da parte dei soggetti che interagiscono attraverso Internet (fornitori di rete, fornitori di servizi di telecomunicazioni, *providers*), dirette entrambe ad individuare forme di responsabilità specifiche per ciascun soggetto.

In questo contesto, si è fatta da tempo strada la possibilità di una terza via, ribadita in un articolo del dottor Buttarelli: la Commissione europea ha cioè ipotizzato una carta internazionale, alla cui stesura diano un contributo parti private e gruppi sociali. Più che una "terza via", la individuazione di un nucleo duro di princìpi a livello internazionale appare tuttavia il presupposto di qualunque soluzione si voglia adottare su questo tema.

Vengono poi in considerazione strumenti che garantiscano la sicurezza del trattamento dei dati, anche dal punto di vista dell'utente, quali sistemi di protezione, cifratura delle trasmissioni (con individuazione dell'autorità che deve conservare le chiavi per decrittare i messaggi stessi), modalità di accesso anonimo alla rete, e così via.

Quanto a tale aspetto, l'attenzione, anche in sede europea, notoriamente si è spostata dall'uso degli strumenti crittografici alla individuazione di requisiti a monte, che evitino la creazione delle tracce digitali, lasciate dalla consultazione dei siti Internet (penso alla direttiva 97/66 UE in materia di telecomunicazioni; alla raccomandazione 3/97 del gruppo per la tutela della vita privata, con riguardo al trattamento dei dati privati, adottata nel dicembre '97; alle conclusioni della Commissione ministeriale di Bonn, del luglio '97, ed alle linee guida per il trattamento dei dati personali per Internet, in corso di adozione da parte del Consiglio d'Europa). La soluzione dell'anonimato - mi piace ricordarlo - è stata proposta da ultimo nella relazione per il '97 del Garante per la protezione dei dati.

La situazione si complica ulteriormente appena si pensi che, in senso contrario, è invece necessario garantire un controllo sui *newsgroup* (e cioè sui siti Internet dedicati ad argomenti particolari, cui accede un numero aprioristicamente indeterminabile di fruitori, senza che tale accesso sia differenziabile), così da assicurare la identificabilità di coloro che contribuiscono al sito, fornendo la relativa documentazione: e ciò in vista della tutela delle categorie "deboli", come ad esempio i minori (penso a tutte le tematiche che sono in questo momento particolarmente sentite, non solo in Italia, sul rapporto tra pornografia, sfrutta-

mento dei minori e Internet). Risulta insomma particolarmente forte, nella materia in esame, l'eterna dialettica degli interessi contrapposti (il diritto dell'informazione, da un lato, e la tutela della riservatezza, dall'altro lato) e la conseguente difficoltà di individuare soluzioni normative rigide e risolutive a livello legislativo, alla cui previsione si oppone, inoltre, la necessità di predisporre soluzioni omogenee e quindi concordate a livello internazionale, come pure imposto dalla dimensione transfrontaliera della comunicazione mediante le reti Internet e dalla altrimenti facile eludibilità di singole discipline nazionali.

A livello di soluzioni normative, nel quadro della prevenzione (in senso lato), lo strumento certamente più duttile e di più agevole formazione sarebbe, nel contesto dei princìpi internazionali che si andranno affermando, la autoregolamentazione.

Solo in seconda battuta, e nel quadro di riferimento che si sarà formato a livello internazionale ed a livello di autoregolamentazione, sarà utile l'intervento dello Stato, al fine di elaborare gli strumenti di individuazione delle responsabilità.

In questo senso, dal documento finale della Conferenza ministeriale (punto 41) emerge l'impegno dei Ministri - e ci riteniamo vincolati a questo impegno - a una definizione precisa delle norme giuridiche in materia di responsabilità delle parti "nell'intera catena, che va dalla creazione all'utilizzo di contenuti". In esso si trova specificato, inoltre, che le norme in tema di responsabilità per i contenuti dovrebbero basarsi su una serie di princìpi comuni, tali da garantire condizioni paritarie in base alle quali gli intermediari, i gestori di rete, nonché i fornitori di accesso non dovrebbero, in linea di massima, essere responsabili dei contenuti, dovendosi per contro valutare "se tali intermediari abbiano ragionevole motivo di conoscere i contenuti in oggetto e siano ragionevolmente in grado di controllarli".

Vorrei solo sottolineare come il problema della responsabilità del *provider* si complica enormemente solo che si pensi alla necessità di soluzioni normative, differenziate a seconda del tipo di servizio che di volta in volta viene preso in considerazione nonché, nell'ambito dello stesso tipo di servizio, in base alla diversa gravità degli illeciti commessi via rete (si pensi ai siti per pedofili, in relazione ai quali la possibilità di ipotizzare una corresponsabilità del gestore, secondo uno schema di responsabilità per omesso controllo a titolo di colpa, analogo, ad esempio, ad un istituto ormai vecchio e consolidato in materia di reati a mezzo stampa, potrebbe essere auspicabile in linea astratta, ma dovrebbe essere verificata alla luce della impossibilità materiale e giuridica, nella maggior parte dei casi, di esercitare questo controllo anticipatamente, o anche in tempo reale).

Gli illeciti ipotizzabili sono svariati; vanno da forme di diffamazione, alla violazione della normativa sul diritto d'autore, alle frodi comunitarie, alla pornografia infantile. Passano attraverso la lesione di interessi a dimensione prevalentemente personalistica, per giungere alla offesa di interessi di natura anche e immediatamente pubblicistica. A questo proposito, penso alle nuove forme di riciclaggio di denaro sporco attraverso le tecniche dei "ciberpagamenti" che rendono possibile l'effettuazione istantanea di operazioni su vasta scala, a distanza e in modo anonimo, evitando l'intervento delle istituzioni finanziarie tradizionali, cui il sistema devolve importanti compiti di controllo. Tali nuovi "prodotti", che sono destinati a sostituire il denaro e ad offrire altri modi per realizzare transazioni, com-

prendono anche i sistemi bancari elettronici, grazie ai quali i saldi attivi disponibili, amministrati da un personal computer, sono trasferiti elettronicamente attraverso le sedi Internet.

Ciò vuol dire che ci troviamo di fronte ad approcci tecnologicamente completamente nuovi. In un certo senso si ripete quello che è capitato nel campo della privacy più in generale: siamo costretti a ripensare e a rimeditare completamente, alla luce dell'evoluzione tecnologica, diritti che pure sono di elaborazione recentissima.

Penso, in particolare, al tema che mi vede molto vicino per ragioni di studio precedente e di interesse attuale: e cioè alla lotta al riciclaggio del denaro sporco, lotta iniziata ancora di recente (risale agli anni '80 e '90), ma che si è scontrata con una tecnologia la quale ha ampiamente superato le prospettive con fatica individuate negli anni passati.

Anche sotto questo profilo si conferma, dunque, la complessità di questi temi e la necessità di predisporre sistemi normativi adeguati, per quella famosa conciliazione, per il contemperamento degli interessi. Emblematica, su questo punto, la giurisprudenza della Corte europea dei diritti dell'uomo nella quale, con riguardo a settori di comunicazione più tradizionali e meno complessi di Internet, è stato da tempo sviluppato un principio, che io penso sempre valido, di "proporzione" tra le finalità perseguite dalle restrizioni e i diritti fondamentali, principio che è e deve essere alla base di ogni settore della legislazione, ma tanto più importante in una materia che, come questa, appare in costante ed incessante evoluzione.

In conclusione, il ritardo dell'Italia nell'elaborare la normativa sulla *privacy* si è paradossalmente risolto in un vantaggio - raccolgo qui la sfida del nostro moderatore -, avendo consentito una maggior vicinanza alla piattaforma di princìpi contenuti nella direttiva comunitaria del 1995 (n. 46). È stato detto - e lo confermo - che verso la sua attuazione ci stiamo ancora muovendo (e molto dovremo ancora muoverci): è stato di recente approvato dal Consiglio dei Ministri un decreto legislativo in materia di telecomunicazioni; presso il Consiglio di Stato si trova il regolamento che disciplina le misure minime di sicurezza da osservare per il trattamento dei dati personali. Le previsioni contenute in quest'ultimo sono solo in parte applicabili al trattamento dei dati attraverso Internet (soprattutto per quanto concerne la sicurezza dei dati trasmessi attraverso le reti, o conoscibili mediante l'attivazione dei collegamenti).

Certamente, un'occasione importante sarà rappresentata dall'attuazione della legge 676 del '96. In quella sede dovremo dettare una normativa, sia pure minimale, delle responsabilità e dei diritti nel mondo di Internet e studiare i modi migliori per sollecitare forme di autoregolamentazione sul versante della prevenzione.

Siamo di fronte ad una delle tante sfide che mi sembra giusto ricordare oggi, giorno della festa dell'Europa, e che credo vada affrontata in una dimensione veramente globale (a Washington in dicembre, nell'incontro del G7/P8, abbiamo posto sul tappeto il problema degli *high-tech crimes*, con una particolare urgenza e con una particolare consapevolezza).

Mi sembra importante, nel giorno della prima festa dell'Europa, sottolineare questo aspetto, come messaggio di speranza: in fondo, nella prospettiva di un'Europa che non sia soltanto delle monete, della finanza, nell'Europa dello spazio giuridico comune,

nell'Europa del terzo pilastro, nell'Europa delle istituzioni, in una prima sfida, quella globale contro la criminalità organizzata, si sono già fatti dei grandi passi avanti.

Adesso si tratta di vincere la seconda sfida, che va dalla repressione e dalla responsabilità, alla prevenzione, alla valorizzazione del diritto alla personalità.

Mi pare, questo, l'augurio migliore che posso fare; rinnovo il ringraziamento per i lavori del vostro incontro, che certamente daranno un contributo positivo, oltre che impegnativo in relazione a ciò che tutti insieme abbiamo ancora da fare.

Grazie.

Prof. Ugo De Siervo

Ringraziamo caldamente il Ministro che, come abbiamo tutti sentito, è entrato puntualmente in molti dei temi che in parte avevamo affrontato anche noi.

Con l'intervento del Ministro e, chiedendo scusa a chi si era iscritto a parlare ed a cui, per ragioni di tempo, non è possibile dare il microfono, riteniamo chiuso il quinto passaggio del nostro convegno.

Tra pochissimi minuti daremo inizio al finale scambio di opinioni tra i componenti del Garante, insieme al professor Roberto Zaccaria, Presidente della RAI, sulle prospettive legislative e su altri problemi dinanzi ai quali ci troviamo.

TAVOLA ROTONDA

Prof. Stefano Rodotà

Riprendiamo il lavoro per questo scambio di opinioni finali, al quale abbiamo il piacere di invitare a partecipare il Presidente della Radio Televisione, Roberto Zaccaria, che ringrazio particolarmente.

Questo scambio di opinioni finali è certamente arricchito dalla sua tripla esperienza: di studioso, di membro del Consiglio di Amministrazione della RAI per molti anni, e quindi conoscitore non solo di un'azienda, ma del modo in cui i problemi della comunicazione si sono venuti evolvendo in Italia.

Oggi ha la responsabilità non piccola di essere alla testa di questo settore particolarmente importante per la vita civile. Lo ringrazio di nuovo e gli passo la parola.

Prof. Roberto Zaccaria

Ringrazio il Presidente Rodotà e tutta l'Authority. Sono legato, anche per ragioni personali, a molti dei presenti e ho seguito i lavori con grande interesse. Per queste ragioni mi accosto a questa materia con un particolare stato d'animo.

Per preparare queste note di lavoro abbiamo cominciato col mettere nel computer della nostra banca dati, distintamente, le due voci che riguardavano l'oggetto di questa riunione. Anzitutto abbiamo digitato la parola "Internet" ed abbiamo trovato una quantità enorme di documenti, di testi e di riferimenti; abbiamo poi inserito la parola "privacy", e abbiamo letto una quantità ancora maggiore di informazioni e di documenti.

I miei collaboratori hanno poi osservato che io avrei dovuto parlare in questa sede come Presidente della RAI, ragione per cui abbiamo messo "RAI", e si può ben immaginare la "risposta" del computer.

A quel punto, si è pensato di mettere le tre parole insieme: Internet, privacy e RAI. E non è venuto fuori quasi niente. Credo che questo sia un fatto positivo perché vuol dire, o almeno così io ho inteso, che questi tre elementi insieme debbano portare alla riflessione, porre dei problemi, più ancora che soluzioni predefinite.

Mi sia ora consentito un accenno autobiografico. Penso possa servire per capire il

genere di problemi che ci troviamo ad affrontare. In realtà, tra le poche informazioni che erano venute fuori richiamando insieme Internet, RAI e privacy, ve ne era una che nei giorni precedenti mi era stata già segnalata: la presenza cioè di un sito Internet che collegava il mio nome ad una iniziativa di un Comitato politico del 1994.

Qualcuno si è preoccupato per quello che avrebbe potuto dire la stampa a seguito del fatto che in un sito Internet si venisse a conoscenza che il Presidente della RAI era stato responsabile di un gruppo che faceva attività politica. Ai giornalisti presenti dico che non mi sono preoccupato allora e non me ne preoccupo oggi in quanto, fino a prova contraria, avere avuto delle idee politiche, o averle ancora, sono dati sensibili, ovviamente, ma sono dati che la gente ha diritto di conoscere, se riferiti a chi riveste certe posizioni.

Questo fatto mi ha però fatto riflettere che quando un sito viene attivato e poi abbandonato negli anni, può creare problemi, nel senso che è un po' come quelle cose che non si spolverano frequentemente, che restano lì e col passare del tempo possono acquistare un significato diverso.

Passando a delle riflessioni un po' più, non dico organiche, perché non ho questa pretesa, ma più meditate, vorrei considerare un argomento che in questa sede mi sembra sia stato affrontato poco, ne ha fatto cenno soltanto Pace in un rapido intervento.

Mi riferisco al profilo di impostazione costituzionale che appartiene alla mia esperienza universitaria e che fa sì che il problema, in generale collegato ai nuovi mezzi di comunicazione e in particolare a mezzi come Internet, caratterizzati da una forte polifunzionalità, renda necessaria una nuova riflessione costituzionale. Capire cioè se l'inquadramento ed il governo di questo fenomeno possa avvenire nello schema dell'articolo 21 o in quello dell'articolo 15.

Si tratta di un problema che i costituzionalisti affrontano già da alcuni anni, e che sta diventando particolarmente acuto, perché certamente i tradizionali canoni di distinzione tra la comunicazione da punto a massa, e la comunicazione da punto a punto sono saltati nettamente. Probabilmente ormai, tra l'articolo 21 e l'articolo 15 la lettura non può essere fatta che insieme, ed anche il concetto di determinatezza, che una volta consentiva di distinguere l'ambito di applicazione di una norma costituzionale rispetto ad un'altra, è fortemente in discussione.

Ci sono una serie di servizi, di attività, di funzioni - e appunto quelle collegate ad Internet ne sono un esempio molto significativo - che consentono di volta in volta un inquadramento, in alcuni casi anche con dubbi significativi, nell'articolo 21, che potrebbe essere quello che più direttamente può riguardare il problema dei siti, o nell'articolo 15, che è la comunicazione intersoggettiva.

Devo dire però che ancora siamo ad analizzare tutte le potenzialità del fenomeno, perché accanto ai vari servizi più nitidamente inquadrabili nell'uno o nell'altro genere, vi sono delle attività che si collocano in posizione intermedia. Si è di fronte ad un problema non soltanto teorico, perché abbiamo ascoltato dal Ministro Flick quale sia la serie di problemi collegati alla regolamentazione anche sovranazionale.

Nel corso dell'ultima sessione, coordinata da De Siervo, si è parlato del rilievo dell'au-

todisciplina in questo campo, ma non vi è dubbio che noi, soprattutto quando dobbiamo valutare le soluzioni di tipo regolamentare, che si pongono con prudenza in questa materia, dobbiamo avere ben chiaro che il trattamento è diverso a seconda che ci ricolleghiamo all'articolo 21 o all'articolo 15.

Tanto per fare un esempio, l'articolo 15 richiama in maniera precisa i profili della segretezza, mentre quelli relativi al buon costume, richiamati dall'articolo 21, nell'articolo 15 hanno un richiamo non specifico, che dà adito ad altri tipi di soluzioni interpretative.

Questa premessa a mio avviso è importante, perché ogni soluzione che andremo a trovare, poi dovrà essere misurata con questi parametri costituzionali, e probabilmente dovremo andare verso una sorta di rilettura complessiva di questo momento, attraverso un combinato disposto delle norme 21 e 15, che legga la libertà della comunicazione come un tutto uniforme, e però lasci intravedere quelle particolari garanzie che l'articolo 15 riserva alla comunicazione, che una volta si definiva intersoggettiva.

Noi sappiamo bene che lo sviluppo di Internet, la maggiore velocità della trasmissione, la banda di utilizzazione, consentiranno in futuro di veicolare con qualità praticamente indistinta rispetto a quella attuale, il mezzo televisivo attraverso questa rete. D'altra parte già oggi in qualche misura, proprio utilizzando i siti Internet, molti ascoltano, ad esempio, i giornali radio locali. Ad esempio, si può sentire al Nord il giornale radio della Campania. In questo modo già si realizza un meccanismo di comunicazione potenziata ad utilizzazione personalizzata.

Ebbene, devo dire che, dal punto di vista della RAI, quando essa utilizza Internet come strumento di informazione, e quindi come rete di distribuzione, non pone problematiche nuove rispetto a quei problemi generali di cui ho parlato prima, che sono la tutela del buon costume, la riservatezza, e che riguardano limiti tradizionali nei confronti della professione giornalistica.

Vi è poi un profilo diverso, quando cioè la RAI utilizza Internet per lo scambio di dati e informazioni. La cosa riguarda non soltanto la rete Internet, ma anche Intranet, un tipo di comunicazione che si sta potenziando molto. Anche in questo caso si pongono i tradizionali problemi di sicurezza delle comunicazioni elettroniche, ed ancora una volta ricordo le problematiche legate alla cifratura e alla firma digitale, di recente disciplinate dal DPR del novembre 1997.

In questa chiave, ancora una chiave tradizionale, la rete serve alla RAI per potenziare i propri compiti di servizio pubblico, soprattutto per quel che riguarda il diritto all'informazione, problematica messa bene a fuoco dai giudici costituzionali.

Il servizio pubblico ha questo impegno significativo nei confronti dei cittadini, ed il diritto all'informazione sta diventando un'espressione sempre più cogente e pregnante, sicché, ad esempio, in materia di informazione ambientale, praticamente si è in presenza della costituzione di un vero e proprio diritto soggettivo. E vorrei dire che, grazie all'utilizzo di strumenti ulteriori, come appunto Internet, la RAI potrebbe contribuire ad accrescere l'effettività del diritto in questione, mettendo a disposizione di un pubblico sempre crescente un'enorme quantità di informazioni a costo zero.

Si tratta di una possibilità da tenere presente, come è da tenere presente che la stessa Comunità Europea, nel Libro Verde sulla convergenza del dicembre del '97, anche se soltanto in un piccolo inciso, ha riconosciuto che "l'impatto della convergenza potrebbe influire sul modo di ottenere gli obiettivi di interesse pubblico, tradizionalmente collegati al servizio pubblico". Inoltre, cito ancora testualmente dal Libro Verde: "Ai concetti ed alle finalità proprie del servizio pubblico finiscono con il sovrapporsi quelli relativi al servizio universale. La possibilità di offrire servizi di telefonia vocale via computer e TV, o di usare Internet per leggere, guardare e ascoltare programmi delle emittenti televisive, indica che le nuove piattaforme potrebbero svolgere un ruolo nel soddisfare tali obblighi".

Questo è un primo, importante terreno di riflessione, un terreno sul quale noi abbiamo una sorta di problematica tradizionale, che viene in qualche modo valorizzata, che viene accentuata dalla possibilità di utilizzare questi mezzi.

Vi è però un profilo particolare, legato a privacy e RAI - in questo caso Internet non c'entra, a testimonianza delle difficoltà a trovare temi in cui c'entrino le tre parole chiave - in relazione al quale abbiamo avuto qualche problema, collegato al fatto di essere noi, questa volta, non soggetti, ma oggetto di informazione.

Vi è stata anche qualche polemica al riguardo, quando, durante una riunione di lavoro del Consiglio di amministrazione, fuori dalla Rai, in un luogo da noi considerato privato, siamo stati osservati con particolare attenzione da parte di alcuni giornalisti. Avevamo avuto la preoccupazione, infatti, che da un'osservazione un po' troppo ravvicinata, in luoghi non propriamente pubblici, noi potessimo ricevere un danno, o potessero averlo alcune persone "toccate" da quell'informazione. Ci preoccupava, soprattutto, il trattamento dei dati, che è un tema tipico dell'Autorità.

Debbo dire che recentemente abbiamo voluto chiudere la questione con una sorta di scherzosa battuta, rimanendo però fermi nella convinzione che il problema esiste, nel senso che anche i mezzi di informazione debbono avere la consapevolezza che c'è un limite al di là del quale anche soggetti a forte rilevanza pubblica e quindi con responsabilità di trasparenza, possono avere il diritto a riunirsi privatamente.

Abbiamo comunque voluto ritirare - è una notizia che do ai giornalisti presenti, scusandomi per il fatto che può interessare una parte molto ridotta del pubblico - i due esposti presentati, relativi a una possibile violazione della privacy nell'esercizio di un'attività collegata all'informazione. Ritirando l'esposto presentato, credo che abbiamo anche contribuito a rendere più snella l'attività del Garante. Il problema resta, ma lo discuteremo in altra sede.

Vi è da fare ancora qualche considerazione, in relazione al tema di cui si sta discutendo. La RAI ha una serie di obiettivi, che molto rapidamente ricorderò, ed uno di quelli primari, nel suo percorso di rinnovamento tecnologico e comunicativo, è quello relativo all'utilizzo di strumenti che consentano un accesso sicuro ad una serie di nuovi servizi. Non parlo tanto delle pagine dei siti RAI più conosciuti, che evidentemente chiunque può utilizzare, ma mi riferisco in particolare ad un progetto molto importante, denominato "Teche".

A questo punto si impone una riflessione, anche con riferimento ai tre termini che ho citato all'inizio. La RAI ha un ambizioso e importante progetto che riguarda le teche, un

patrimonio straordinario dell'audiovisivo italiano, e si ricollega ad altri analoghi in diversi Paesi.

Questo progetto, in gran parte interno, consentirà nel tempo di accedere - e già in parte oggi lo consente, essendovi un sito dedicato - attraverso certe pagine, ad un catalogo che si arricchirà progressivamente e, nel giro di pochi anni, consentirà una ricerca estremamente puntuale di tutta una serie di programmi e documenti che la RAI ha nei suoi archivi. Il progetto consentirà agli stessi operatori RAI, ma anche a soggetti esterni, per ragioni di studio o di documentazione, di andare a recuperare tutti questi materiali.

Sono previsti almeno tre livelli di possibile accesso. Un primo livello sarà aperto al pubblico in generale e permetterà, attraverso una consultazione più rapida di alcune pagine, di accedere ai documenti ed ai materiali individuati.

Un secondo livello, che si potrebbe definire intermedio, sarà utilizzabile da alcuni centri specializzati, quali biblioteche, istituti universitari, centri di ricerca; esso prevederà per l'accesso l'uso di una parola chiave e consentirà ad una serie di operatori di entrare in un catalogo di dimensioni smisurate, che oggi siamo già in grado di apprezzare e valutare.

Il terzo livello sarà quello dell'utilizzazione a fini di produzione, per cui chi deve realizzare un servizio può andarsi a prendere, ad esempio, un'intervista di Rodotà di qualche anno fa, utilizzando contemporaneamente nella ricerca la possibilità di puntualizzare esattamente il fotogramma, il testo, le parole che accompagnano l'immagine.

Va detto che ci siamo posti il problema che può derivare dal prelievo da questa enorme banca dati di una serie di documenti o di immagini che possono contenere anche dati sensibili.

Si pensi, infatti, che si sono avute intere serie di programmi di informazione, o di fiction, e che molti sceneggiati hanno interessato problemi di minori. Io ricordo, negli anni passati, tante discussioni legate alla messa in onda di alcuni programmi, alla scelta di trattare le vicende private di giovani, o di mandare in onda alcuni grandi processi.

Tutto questo potrebbe essere controllato nella messa in onda, ai fini di quel diritto all'oblio di cui si è spesso parlato. Ma se noi abbiamo una garanzia attraverso la messa in onda, nel senso che possiamo controllare, ogni qualvolta ritrasmettiamo qualche programma, che questo sia coerente con le nuove regole che si stanno precisando in questa materia (mi riferisco alla legge sulla tutela della *privacy* e dei dati personali), il discorso è più complesso con riferimento alla riutilizzazione.

Ho detto che vi sono tre livelli di utilizzazione di questi archivi, il primo riguarda coloro che realizzano i programmi e che hanno una sorta di nuova responsabilità editoriale; un secondo, si riferisce a coloro che consultano le pagine generali, dove sarà più difficile l'accesso a questi dati; infine, una fascia intermedia, dove comunque si può andare a scartabellare negli archivi, prelevare dati o informazioni che potrebbero essere oggi, diversamente da allora, quando non esisteva l'attuale normativa, in contrasto con certi parametri.

Non sto certo dicendo tutto questo per rendere più difficile il compito delle molte persone, alcune delle quali sono qui presenti, che stanno lavorando a questo che io reputo uno straordinario progetto. D'altra parte, il Presidente Rodotà, quando ha presentato il rapporto ha chiaramente sottolineato lo spirito che informa l'attività del Garante: noi

siamo qui per tutelare alcuni valori, non per complicare le cose o per inserire degli elementi e dei passaggi "burocratici".

Noi abbiamo già semplificato molto, però è forse necessaria un'ulteriore, approfondita riflessione. Andare a rivisitare il nostro patrimonio audiovisivo ha un valore straordinario in termini culturali, non soltanto per il nostro Paese, ma anche per tutti quei Paesi che, attraverso questo patrimonio, possono resistere ad una invasione che viene dai nuovi mezzi e dalle nuove tecnologie.

Occorre però riflettere quanto questa riscoperta possa richiamare l'attenzione su una serie di dati, anche sensibili, che oggi sono oggetto di particolare attenzione, e che invece ieri non lo erano nella stessa misura.

Oggi abbiamo il valore aggiunto della riscoperta, ma lo dobbiamo gestire alla luce dei nuovi princìpi.

Nel dare un contributo alle riflessioni di queste giornate di lavoro e nell'affermare che la RAI sta facendo molte cose, non ho voluto però fare semplicemente un'operazione di pubblicizzazione e di divulgazione di iniziative in corso.

Ho voluto dire che la RAI è sì impegnata in un grande lavoro, ma valuta - e lo stiamo facendo con grande attenzione - in che misura i valori di cui qui si discute, come il rapporto fra Internet, privacy e possibilità di accesso agli archivi, possano confliggere o contemperarsi con le iniziative in atto, di grande spessore anche d'impresa.

Ringrazio per la possibilità che mi è stata offerta di partecipare ai lavori e di intervenire in prima persona.

Prof. Stefano Rodotà

Desidero ringraziare il Presidente Zaccaria ed assicurarlo subito che le questioni importanti che ha segnalato, in particolare nel momento finale del suo intervento, noi abbiamo cominciato a porcele, essendo già emerse durante questa fase piuttosto tormentata, che ha riguardato l'elaborazione del codice deontologico dei giornalisti, una vicenda che qualcuno ha avuto, credo, interesse a drammatizzare, ma che mi sembra si sia poi conclusa in modo felice.

È reale il problema dell'utilizzazione delle grandi raccolte di informazioni, e particolarmente delicato appare quello relativo alle immagini, perché nella ripresa di una folla, la possibilità di rintracciare uno spettatore a distanza di anni certamente pone qualche problema.

Sulla questione credo che si possa comunque riflettere in modo positivo, nel senso che quel bilanciamento e quell'equilibrio tra valori costituzionali, che Roberto Zaccaria sottolineava fin dall'inizio, è nelle corde stesse della legge n. 675, che si apre proprio all'insegna non solo di un riferimento alla riservatezza e all'identità, ma ai diritti e alle libertà fonda-

mentali, imponendo quindi fin dalla sua apertura questa delicata questione.

Appare, a mio avviso, importante nella dimensione generale questo lavoro della RAI, finalizzato ad accrescere la massa critica di informazioni disponibili per i cittadini. In numerosi interventi di queste due giornate e nel mio stesso, all'inizio dei lavori, è stata opportunamente messa in evidenza la connessione tra valori di democrazia non agganciati al gioco troppo facile del "sì" e del "no" di qualche sondaggio o di qualche *referendum* istantaneo, e la creazione della massa critica a disposizione dei cittadini.

In merito alla notizia relativa alla rinuncia ai ricorsi presentati al Garante, va detto che quando uno viene liberato da un lavoro, soprattutto da un lavoro difficile, è sicuramente contento. Vorrei però precisare che porci questioni difficili - e devo dire che ne vengono poste ogni giorno - è la parte più impegnativa ma anche più stimolante di questo lavoro.

Noi non arretriamo di fronte ai problemi che ci vengono posti, ed ai quali dobbiamo rispondere, non solo per ragioni di ufficio, ma per una esigenza nostra personale.

Vorrei a questo punto richiamare le parole di Mario Monti, su una questione che è anche entrata nella discussione di questi due giorni. L'avere scelto, in alternativa al ricorso al giudice ordinario, la possibilità di rivolgersi al Garante, ha un significato di accrescimento dei poteri reali del cittadino.

Costi bassi o inesistenti: abbiamo risposto a problemi che ci sono stati posti addirittura per telefono. Rapidità: in merito abbiamo dei problemi, che sono legati anche alla enorme quantità di questioni che abbiamo dovuto affrontare ed alle ristrettezze dell'organico; credo comunque che, rispetto ad ogni altra istituzione, quanto a rapidità i nostri tempi di risposta siano paragonabili solo a quelli della Corte Costituzionale, in qualche momento della sua storia. Non va poi trascurato l'aspetto della semplicità di rapporto e di trasparenza, alla quale il Garante ha ispirato la sua attività.

Quindi, le sollecitazioni non solo non ci disturbano, ma ci aiutano. Vorrei aggiungere che non ci disturbano neppure le critiche. Quando si segnala qualche settore dove qualcosa non funziona e crea difficoltà soprattutto ai cittadini, noi stiamo attentissimi. Quello che qualche volta ci disturba è la prospettazione parziale delle questioni, per cui viene considerato un problema magari reale, per negare nella sua globalità il senso del lavoro che stiamo facendo. Tra l'altro, trovandoci noi sulla frontiera dei diritti dei cittadini, cioè dei diritti di 57 milioni di italiani, questo sembra essere un cattivo servizio reso all'opinione pubblica.

È stato detto dai giornali, ad esempio, che questa legge non funziona, perché ha risposto soltanto il 20 per cento dei clienti delle banche. Riflettendo sul fatto che i clienti delle banche sono stimati ad una ventina di milioni, e considerato che molti sono clienti allo stesso tempo di più di una banca, si scende a 15 milioni, il 20 per cento dei quali sono 3 milioni di cittadini italiani che hanno risposto, nella maggioranza dicendo che non vogliono avere, ad esempio, materiale pubblicitario a casa.

Io non discuto il fatto che il problema esiste, ma ritengo straordinario, dal punto di vista quantitativo e qualitativo, che milioni di persone che fino a quel momento non avevano voce, abbiano potuto dire, magari su una questione che può essere banale e che pone certamente problemi al sistema bancario, quello che vogliono fare dei propri dati.

È proprio a questa distribuzione sociale di potere che noi siamo attentissimi. Non siamo i custodi di un nostro piccolo privilegio, ma stiamo cercando di rendere tutto più fluido. Se arriva una cattiva informazione, i canali diventano meno fluidi, pertanto io sono grato anche per questo motivo a Roberto Zaccaria per le cose che ci ha detto.

Vi infliggiamo ancora per pochi minuti la nostra presenza, perché ci sembra utile, proprio in questo spirito di trasparenza, non solo offrire a chi ha seguito questo convegno una qualche riflessione da parte delle quattro persone che costituiscono l'Ufficio del Garante per la protezione dei dati personali, ma anche dare una volta di più un piccolo contributo alla trasparenza del lavoro di un ufficio, che si realizza anche attraverso la possibilità di un contatto diretto con le opinioni di ciascuno dei componenti di questo stesso ufficio, con lo stile, con il modo in cui ciascuno di noi affronta le questioni.

L'ora è tarda, ma credo che qualche valutazione finale ce la consentirete. Io di tempo già ne ho preso tanto, per cui da parte mia vi saranno solo poche parole di saluto alla conclusione dei lavori; ma immediatamente il Presidente Santaniello ci dirà la sua.

Prof. Giuseppe Santaniello

Io vorrei riprendere brevemente in considerazione il problema della tutela della proprietà intellettuale, ma non per ripetere i criteri che in maniera così completa ed efficace sono stati analizzati ieri, a proposito di Internet.

Vorrei per un momento trasporre nella situazione italiana i criteri ed i valori che riguardano Internet, sia in relazione alla situazione legislativa del nostro Paese, sia per quanto riguarda in particolare il comportamento dei *media* di fronte all'inquadramento ed alla soluzione dei problemi di tutela della proprietà intellettuale, con speciale riguardo al settore comunicativo.

Oggi, infatti, i diritti d'autore, che sono nati storicamente per la tutela del pensiero scritto, si sono ampiamente diffusi, potenziati, moltiplicati, attraverso l'attività mediale.

Ritengo che il tema della proprietà intellettuale e della sua tutela riguardi tre aree, delle quali una ieri è rimasta in ombra. Le tre aree sono quelle della libertà di concorrenza e di mercato; della libertà del settore comunicativo; vi è poi l'area che si incentra nel diritto alla riservatezza.

Ora, che la proprietà intellettuale interessi anche il tema della libertà di concorrenza e di mercato, nonché della salvaguardia di questa libertà, è ormai un dato che è stato ribadito attraverso entrambi gli itinerari che abbiamo tracciato ieri, ossia l'itinerario europeo e quello americano.

Per poter documentare questa affermazione, ricordiamo che nel Libro verde della Comunità europea si dice che bisogna evitare che in una tutela imperfetta, inadeguata,

oppure attraverso una serie di lesioni del diritto di autore, si verifichino distorsioni di concorrenza.

Ma ugualmente tale concezione rimane affermata in un altro documento importante, che proviene (nel luglio 1997) dalla Casa Bianca e riguarda il commercio elettronico. Anche tale documento pone in rilievo l'esigenza di fare in modo che la tutela della proprietà intellettuale sia piena, perché alterando questa tutela, o violando i diritti d'autore, si falsa la concorrenza e quindi il mercato, per cui viene inferta una ferita ad una libertà fondamentale.

Va anche detto che, sempre nel Libro verde, si sostiene che bisogna porre attenzione ad un fenomeno particolare. I fattori dell'economia globale, dell'informazione globale portano ad un forte trasferimento dell'iniziativa imprenditoriale dalla impresa piccola e media alla grande impresa; però questo pone il problema di evitare che si verifichino processi generatori di concentrazioni.

Veniamo al secondo punto fondamentale: l'area di libertà del sistema comunicativo, in relazione al quale il Presidente della RAI Prof. Roberto Zaccaria ha tracciato una serie di profili molto approfonditi e molto chiari. Io però vorrei esaminare come i media italiani si sono comportati di fronte al problema della tutela della proprietà intellettuale, avendo anzitutto riferimento al servizio pubblico radiotelevisivo e poi alla emittenza privata.

Orbene, proprio dall'esame di questi settori fondamentali, noi traiamo alcuni elementi di riflessione, a partire dalla valutazione delle modalità con le quali il sistema mediatico applica la legge di protezione del diritto d'autore.

Questa legge, come è noto, risale al 1941, quindi è legata a presupposti e condizioni cristallizzate in quel tempo e che oggi perdono molto della loro validità ed efficacia. La concezione della tutela del diritto di proprietà intellettuale, del 1941, era nettamente dominicale e proprietaria del diritto d'autore. Essa divideva il diritto d'autore in due profili fondamentali: il diritto della personalità, ossia il diritto morale dell'autore, ed il diritto patrimoniale.

Per quanto concerne la patrimonialità, può ancora ritenersi intatto quell'impianto normativo; ma il punto fondamentale (il diritto di personalità, il diritto a divulgare l'opera) si è invece profondamente modificato, essendo nato in un momento legato fortemente alla territorialità.

Ricordiamo tutti che il 1941 era ancora un anno della chiusura del Paese italiano a tutte le grandi correnti di pensiero e di traffico, mentre ora è mutata profondamente questa concezione. La paternità dell'opera è immutata, ma la divulgazione dell'opera, proprio attraverso i media, ha avuto tale una dilatazione e tale un'espansione, per cui quella normativa non regge più all'impatto dei problemi che sono sopraggiunti.

Ma sono variati anche i contenuti formali e sostanziali del diritto d'autore e della tutela del diritto d'autore. È da considerare che nell'immaginario tradizionale l'autore era l'artigiano che crea la propria opera in solitudine, e sulla base di materiali totalmente originali.

Ma che cosa avviene nel mondo mediale e multimediale moderno? I nuovi prodotti e i nuovi servizi sono il risultato di una pluralità, e talvolta di una coralità di individui, "il cui contributo personale è spesso difficilmente identificabile". Dice il documento, con un'anali-

si raffinatissima, che ormai il diritto d'autore, attraverso l'enorme potenziamento dei media, addirittura tende quasi a spersonalizzarsi.

Il problema che pongo è come i media hanno interpretato tutto questo. Mi domando se essi sono effettivamente riusciti a tutelare la proprietà intellettuale, anche in questa nuova dimensione.

Questo problema, del resto, viene posto anche nel documento della Comunità europea, quando afferma che l'opera protetta dal diritto di autore evolve in una direzione meno personalistica e più relativa, in ragione di tante caratteristiche connesse all'intervento multimediale.

Tra l'altro, oggi l'opera che viene mediatizzata, viene veicolata dalle reti sia globali che non globali, frequentemente è la *contaminatio* (nel senso latino del termine), vale a dire che è l'incrocio, l'intreccio, il mix (tanto per usare un termine di moda) di tanti prodotti intellettuali, eppure il responsabile dell'emittenza pubblica o privata deve garantire la tutela del diritto di proprietà intellettuale.

Sono questi, a mio avviso, i punti fondamentali. Ovviamente, sono proprio quei temi che i relatori hanno individuato ragionando di Internet, e che si riflettono nella situazione italiana, in quanto non si può sradicare la nostra posizione legislativa da tutto il contesto europeo ed internazionale, nel quale ci muoviamo, con adesione ai princìpi della direttiva comunitaria e anche ai princìpi dei documenti programmatici di matrice americana.

In questa sede di confronto tra le varie *Authority* mi sembra utile proporre che si costituisca un comitato di studio con la presenza delle diverse *Authority*, in rappresentanza sia del mercato e della concorrenza, che del sistema comunicativo.

Ritengo che questa potrebbe essere la via giusta per formulare suggerimenti e proposte, da presentare poi alle sedi competenti e da rendere operative anche nel mondo Internet, con i suoi valori e disvalori, come diceva ieri Yves Poullet, nella faccia visibile e nella faccia non visibile.

Finora, di fronte all'avanzare dei problemi legati al diritto d'autore ed alla sua protezione, soprattutto nel sistema multimediale, in campo legislativo abbiamo prodotto solo scarse regole innovative. L'ultimo portato legislativo riguarda la durata di protezione delle opere postume e delle opere cinematografiche.

Si tratta del decreto legislativo del marzo '97, che poi richiama un altro provvedimento, anch'esso però di raggio limitato, il decreto legislativo 23 ottobre '96 che, dando attuazione alla direttiva 93/86 della CEE, riguardava il coordinamento di alcune norme in materia di diritto d'autore e diritti connessi, applicabili alla radiodiffusione ed alla ritrasmissione via cavo.

Come è facile constatare, il problema di proteggere il diritto d'autore si pone, oltre che nella sede primaria della tutela della riservatezza, anche in altre due sedi molto importanti: la tutela della libertà e della concorrenza, e la tutela del sistema comunicativo.

Prof. Stefano Rodotà

Grazie infinite, anche per il suggerimento operativo, al professor Santaniello, e passo subito la parola all'ingegner Manganelli.

Ing. Claudio Manganelli

Cercherò di essere breve, data l'ora, e forse pochi sono interessati a conoscere il pensiero di un tecnico su questi problemi.

Mi pare che siano emerse, da questi due giorni estremamente densi ed interessanti, alcune linee direttive. Una, come ha detto proprio ieri il Presidente del Garante, Stefano Rodotà, è la necessità di equilibrio tra la tutela dei diritti dell'individuo e le ragioni del mercato. Credo che questo sia il primo punto sul quale è necessario che i componenti del Collegio del Garante riflettano.

Il secondo punto è l'equilibrio tra uno schema di poche regole, magari quelle tradizionali, già oggi in uso, ma evidentemente adattate al nuovo *media*, e l'autoregolamentazione. È noto che possono esservi dei navigatori, o dei fornitori di informazioni, o meglio, coloro che immettono nella rete le informazioni, magari poco educati o eversivi o truffaldini.

Del resto, quando ad esempio vediamo un dipinto murale e un graffito con caratteristiche di armonia e piacevolezza, ci fermiamo a contemplarlo, ma delle scritte o dei disegni osceni neppure ci accorgiamo, e andiamo oltre, senza per questo abbattere il muro o la casa che le reca.

Gli atteggiamenti di tipo censorio che troppo spesso sono suggeriti da varie fonti, dai media, da alcuni politici, francamente mi spaventano. La rete è un luogo - cito ancora le parole di Stefano Rodotà - di infinita libertà e va protetta dagli attacchi, non solo quelli censori, ma anche quelli oligopolistici, e mi pare che il rappresentante dell'Associazione italiana di Internet *provider* ci abbia dato un bel segnale, che non possiamo che riprendere, per elaborare su quella base qualche linea di azione.

Vi è poi un altro aspetto, che è stato poco trattato in questa sede, ma ampiamente sui giornali: Internet 2, che è alle porte. Le preoccupazione è che Internet 2, attraverso una strategia di complessità tecnologiche, possa soffocare Internet, e quindi automaticamente i singoli cittadini che operano in questo villaggio virtuale e vogliono uno spazio libero di cultura, informazione, scambio di messaggi.

Questo è, a mio avviso, un altro problema che l'Europa tutta deve seguire con grande attenzione, perché stiamo parlando di nuove tecnologie, la cui cura è al di là dell'Atlantico.

Pertanto, è indispensabile stare molto attenti.

Si è anche detto che bisogna liberarsi di schemi usuali e pensare in modo concreto a ciò che accade in questo momento, ma anche pensare contemporaneamente a ciò che può accadere. Dobbiamo cominciare a pensare in modo Internet, e pretendere che i nostri legislatori, coloro che nei comitati studiano forme di regole, di norme, di leggi, comincino anch'essi a pensare in modo aperto, in modo Internet.

Bisogna entrare nell'ordine di idee che le regole valide per una comunità non è detto che lo siano per un'altra. La caviglia nuda di una donna, ad esempio, in Islam è proibita, ma sempre in Islam coloro che hanno molti soldi, perché il canale satellitare costa, con un telefono satellitare tranquillamente visitano i siti erotici.

Bisogna pensare Internet e trovare delle regole comportamentali che siano il più possibile interne alla nostra società. Si è parlato di filtri, di responsabilità, e mi pare che il Ministro Flick ci abbia in qualche modo tranquillizzati, perché per parlare di responsabilità di un *provider*, occorre sapere se si sta parlando del *carrier*, oppure del *service provider*, o ancora del *content provider*, che sarebbe ben difficile accusare se affitta spazi ed altri vi caricano dati illeciti.

A noi interessa molto più il problema della privacy, ed io credo che molto si possa fare; ad esempio pretendere che la videata, la schermata che l'utente riceve al momento in cui si collega a un sito, sia chiara e semplice ai fini della privacy. Guai se fosse complessa come l'informativa mandata dalle banche ai clienti; non si capirebbe più niente, ed alla fine il navigatore finirebbe per non connettersi più a quel sito. Deve essere tutto molto semplice, come le cinque righe che abbiamo riportato sul modello di adesione al convegno.

Un'altra preoccupazione emersa stamane è relativa alla *certification authority* che, tra le tante cose, può significare il rischio del monopolio. Se una *certification authority* deve certificare la mia firma come cittadino e come utente della Pubblica amministrazione, mi sembra naturale che sia a cura della Pubblica amministrazione; ma se deve certificare che chi sta facendo, ad esempio, una certa transazione finanziaria è colui che afferma di essere e che sicuramente pagherà, allora non può essere una entità pubblica, ma deve essere, a mio avviso, una entità finanziaria, che si assumerà tutta la responsabilità di verificare l'esattezza e la veridicità dei dati contabili.

Se le strategie - esprimo ora il pensiero di Claudio Manganelli cittadino, e non più componente del Garante - dovessero portare a vincoli e rigidità anche su Internet, come ce ne sono in altri campi e come avviene, ad esempio, col prepagato per i telefonini, oppure quando gli alberghi italiani richiedono il documento di identità, contrariamente a quanto avviene all'estero, in tal caso mi auguro che da qualche parte un *provider* coraggioso attivi un sito, magari *off-shore*, magari su una nave in acque extraterritoriali, magari chiamandolo Sherwood. Sarà buffo assistere agli sforzi delle guardie dello sceriffo di Nottingham che lanciano frecce elettroniche a tutti i piccioni che escono da quel sito, per vedere se hanno nel cilindro il messaggio pornografico, il messaggio antisociale, il messaggio razzista.

Prof. Stefano Rodotà

Io ringrazio Claudio Manganelli, e credo che tutto questo nostro convegno vorrebbe essere un contributo a pensare Internet nel modo giusto.

Prof. Ugo de Siervo

Sono stato colpito positivamente, ma nutro anche una qualche preoccupazione per la semplificazione che tutte le parole comportano, dal fatto che il Commissario Monti ha usato quella bella espressione: "una legislazione leggera" e che successivamente il Ministro Flick ha parlato di "normativa minimale". Come si fa a non essere d'accordo sul fatto che una legislazione debba essere leggera e minimale; il vero problema è però che poi, al di là di tutto, la legislazione, se c'è, deve essere efficace.

Noi sappiamo che questo strumento comporta la necessità di una legislazione essenziale, che poi è snodata sul piano delle normative tecniche o sul piano delle normative categoriali, ma deve essere efficace.

Io, di mestiere faccio il costituzionalista; da alcuni anni studio le fonti del diritto, quindi figurarsi se non sono convinto che sia bene avere leggi brevi e chiare. Questo si dice sempre, poi in realtà le leggi spesso sono brutte ed oscure, perché riferite a fenomeni complessi.

In questo campo ritengo che sia certamente assodato che un forte spazio non può non esistere per normative tecniche, per forme di autodisciplina, ma preferirei parlare di disciplina corporativa. Perché vorrei usare questa accezione diversa? Perché leggendo la legge n. 675 io noto che anche là dove il Garante ha il dovere di stimolare categorie ad adottare codici di deontologia o di buona condotta, come è scritto nella legge, questi codici in realtà non sono pienamente di autodisciplina.

Intanto, essi sono indotti da un'autorità pubblica, che deve vigilare che tali codici siano adottati da soggetti sufficientemente rappresentativi, e addirittura l'autorità pubblica, che in questo caso sarebbe il Garante, con le sue caratteristiche, dovrebbe vigilare che i codici siano adeguati alla legge. È questa la logica in cui noi entriamo.

Condivido quanto ha detto il professor Simitis, e non vorrei che anche per un qualche gioco di parole, o di mancanza di parole, autodisciplina volesse dire che chi è più forte fa la regola. Autodisciplina vuol dire corresponsabilizzazione delle categorie e dei soggetti a regole che essi stessi contribuiscono a dare, e di cui poi garantiscono l'efficacia reale.

Da questo punto di vista, con questa piccola sottolineatura, io ho concluso il mio intervento finale, salvo fare presente che non sono riuscito a capire, nel discorso del Ministro Flick, che pure ci ha detto tante cose, se la delega che va a scadere nel luglio prossimo verrà rinnovata, oppure no. Questa scelta cambia molto: se pensiamo che il Governo della Repubblica debba adottare entro il luglio prossimo la normativa su Internet, allora vorremmo sapere a che punto si è, perché la normativa, specie se vuole essere minimale, leggera, diventa ancora più difficile da scrivere; se invece c'è un tempo maggiore a disposizione, allora potremo forse contribuire tutti a questa migliore, essenziale disciplina.

Prof. Stefano Rodotà

Mi associo incondizionatamente ai chiarimenti opportuni che il professor De Siervo ha dato, per ciò che riguarda le modalità dell'intervento legislativo.

Credo che questi due giorni di discussione abbiano dato un contributo a far cadere quello che il primo giorno io avevo definito un carattere ideologico della discussione, a cominciare dalla contrapposizione tra normativa dura e libertà dell'autoregolamentazione, perché c'è stato un confronto continuo con i fatti, che hanno mostrato come questa contrapposizione in certi casi non esista, secondo quanto ha ricordato Spiros Simitis, rappresentando quello che è accaduto ed accade negli Stati Uniti.

Anche io, nella giornata di ieri, avevo citato il numero cospicuo di casi in cui gli Stati già legiferano o la Federazione americana già si interroga o legifera in materie come il commercio elettronico e la firma digitale. Quindi, le contrapposizioni sono diventate meno ideologiche, il quadro, per ciò che ci riguarda, credo si sia reso più nitido.

Simitis ha evidenziato con grande chiarezza quale debba essere il rapporto tra quadro di princìpi ed autoregolamentazione: una integrazione e non una sostituzione. Naturalmente, come ricordava un momento fa Ugo De Siervo, queste sono semplici enunciazioni; difficile è la traduzione.

Ed allora, lui lo ricordava ed anche io vorrei chiudere su questo tema, che non è solo italiano, si tratta di individuare una disciplina che in questo momento abbia la capacità, non di disciplinare per l'eternità una realtà così mutevole come Internet, ma una disciplina ragionevole, ordinata con ciò che sta accadendo a livello internazionale e sovranazionale, consapevole delle soluzioni nazionali che in questo spazio giuridico europeo che si formerà in ottobre debbono essere tenute presenti.

Questa è la ragione per cui, una volta tanto - non vorrei che ci fossero equivoci -, noi non siamo di fronte a una situazione di inefficienza, per la quale si chiede la proroga di un

rinnovo di una delega semplicemente perché non si è in grado di affrontare un problema, o non ci si sta pensando. Non abbiamo fatto altro in queste giornate, se non altro per la documentazione che è stata distribuita in queste due giornate, si riflette un lavoro ed una preoccupazione costante del Garante, che noi volevamo trasmettere all'opinione pubblica, al Governo, al Parlamento perché ciò che dovrà essere fatto in tempi brevi sia fatto nel modo migliore.

Io non rivelo nulla di particolare, ma noi avevamo proposto, per un decreto che sarà pubblicato tra qualche giorno, di anticipare su alcuni punti delle decisioni. Il Governo ha ritenuto opportuno posporre alcune decisioni, ma su tutta una serie di questioni siamo pronti, prontissimi ad intervenire, a dare attuazione alla delega su punti anche delicati.

La questione è che esistono problemi rispetto ai quali una volta tanto è opportuna una riflessione ulteriore. Io credo che in quest'anno di vita il Garante, con il contributo del Ministro di grazia e giustizia, non abbia mai, lo sottolineo, usato il cattivo costume italiano della proroga dei termini. Tutte le volte in cui abbiamo fatto interventi di questo genere, non era per rimandare a domani quello che si doveva fare oggi, ma semplicemente perché si è ritenuta necessaria una riflessione ulteriore, per vedere come ci si dovrà comportare.

Se noi avessimo puramente e semplicemente differito l'entrata in vigore della legge, come chiedevano in modo un po' miope le categorie interessate, avremmo fatto un cattivo servizio. Sono stati prorogati alcuni termini, nel frattempo la cifra delle notificazioni, stimate in otto milioni, grazie agli interventi che si è potuto mettere a punto è scesa a meno di un milione. Questa è la stima che facciamo: abbiamo liberato sette milioni, tra persone fisiche e persone giuridiche, da un adempimento burocratico. Con tale spirito anche questa volta poniamo il problema.

Da parte di tutti, ci è stato fornito molto materiale su cui riflettere. Noi ci poniamo come tramite verso una serie di altre istituzioni, e possiamo assicurare che davanti all'opinione pubblica continueremo a porre la questione. Non ci sentiamo certo un gruppetto di persone che, investite nel modo più alto da un voto parlamentare, per questo solo fatto, sono depositarie di un potere incontrollabile.

Noi ci confrontiamo tutti i giorni con l'opinione pubblica, e per questo ringraziamo chi è venuto qui, chi ci ha aiutato nell'organizzazione del convegno, chi ha avuto la pazienza ed ha sopportato la fatica di tradurre, per i nostri ospiti stranieri, il linguaggio non sempre semplicissimo che gli specialisti adoperano.

Riteniamo che per noi siano state due buone giornate. Ci auguriamo che siano state utili anche per voi.

Grazie a tutti.

Garante per la protezione dei dati personali

CITTADINI E SOCIETÀ DELL'INFORMAZIONE
Anno II - Supplemento n. 1 al Bollettino n. 5 - 1998

Redazione

Garante per la protezione dei dati personali
Largo del Teatro-Valle n. 6
00186 Roma
Tel. 06 681861
Fax 06 6818650

Pubblicazione della
Presidenza del Consiglio dei Ministri
Dipartimento per l'informazione e l'editoria
Via Po, 14 - 00198 Roma - Tel. 06 85981

Direttore: Mauro Masi

VITA ITALIANA - SCHEDE

Direttore responsabile Mirella Boncompagni

Coordinamento editoriale Laura Musumeci

Progetto e realizzazione grafica Ufficio grafico dell'Istituto Poligrafico e Zecca dello Stato presso il Dipartimento per l'informazione e l'editoria

Stampa e distribuzione Istituto Poligrafico e Zecca dello Stato - Salario

Registrazione Tribunale di Roma n. 298/88