UNIVERSITA' "LA SAPIENZA"

MASTER IN DIRITTO DELL'INFORMATICA E
TECNICA DELLA NORMAZIONE
Anno 2004 - 2005

RESPONSABILITÀ DEI PRESTATORI DI SERVIZI IN INTERNET E TUTELA DI DIRITTI FONDAMENTALI. CENNI AL TEMA DELL'ANONIMATO

Lidia GIANNOTTI

Relatore: Leonardo BUGIOLACCHI

RESPONSABILITÀ DEI PRESTATORI DI SERVIZI IN INTERNET E TUTELA DI DIRITTI FONDAMENTALI. CENNI AL TEMA DELL'ANONIMATO

PARTE I
LA NAVIGAZIONE INTERNET IN EUROPA. DISCIPLINA, OPPORTUNITA' E RISCHI

1. Prime notizie e impressioni su Internet e il tema che ci interessa

Anche se lo strumento è diffuso, soltanto gli addetti ai lavori o i frequentatori più assidui conoscono le regole e le categorie di soggetti che danno corpo e vita alla rete Internet ed alle sue relazioni. Tra questi soggetti ci sono i prestatori di servizi che rendono possibili collegamenti tra un numero enorme di computer.

Alle prime esperienze, la sensazione di essere percepiti grazie ad una tastiera è sorprendente. Più tardi si prende confidenza con la gran quantità di azioni che è possibile compiere una volta diventati esperti, anche più di quelle appartenenti al mondo fisico [1].

Gli strumenti informatici e Internet hanno trasformato la nostra esistenza e rivoluzionato il mercato. Attualmente il commercio elettronico rappresenta solo l'1-2% delle vendite al dettaglio nell'Unione Europea [2]. Ma la tendenza, soprattutto in alcuni settori, è in netta crescita, e comunque la dimensione globale del fenomeno dei contatti, della pubblicità e della circolazione di notizie, immagini e prodotti multimediali è imponente. Così anche i suoi effetti, equiparabili quasi soltanto alla scoperta della stampa a caratteri mobili (che nella seconda metà del '400, grazie alla riduzione di tempi e costi, diede un impulso senza precedenti alla circolazione di libri e conoscenze, modificando tra l'altro l'oggetto che il libro era stato fino a quel momento).

La rete è un "non luogo"; ma quando se ne considerano l'immediatezza e la molteplicità delle relazioni, all'interno di una comunità vastissima e tra infinite comunità, è più luogo degli altri. E la sua novità chiede di riconsiderarne attori e azioni. Nascono numerosi interrogativi, ad esempio, circa le leggi nazionali da applicare e i giudici ai quali sottoporre le controversie. E c'è chi sostiene che gli istituti tradizionali del diritto privato e pubblico, per alcuni profili siano poco adattabili alle nuove esigenze (ad esempio quando si debbano applicare sanzioni di tipo inibitorio), e che sarebbe opportuno pensare ad un nuovo sistema di regole [3].

---

[1] Il rapido spostamento da un sito all'altro, tramite link, ha fatto nascere l'espressione "navigare", immaginando Internet come un oceano sul quale si affacciano una moltitudine di porti.

[2] Dati dell' *Interactive Advertising Bureau,* U.K. 2002 (*www.iabuk.net)*

[3] Tra gli altri, P. SPADA, relazione "*La proprietà intellettuale su Internet*" al convegno "*Cyber law - problemi giuridici connessi allo sviluppo di Internet*", organizzato dall'Associazione italiana giovani

Si "entra" dentro la rete stabilendo una connessione per mezzo di un computer, di un modem di comunicazione e di una chiamata telefonica diretta al *Provider* che fornisce il servizio di connessione. Quest'ultimo verifica i dati di connessione (nome utente e password forniti al momento della richiesta di attivazione del servizio) e assegna all'utente un codice identificativo – indirizzo IP – che consente di conservare anche le operazioni compiute, data e ora. Normalmente i dati identificativi forniti dal richiedente al momento dell'iscrizione non sono oggetto di verifica.

Di tutto questo ci interessa cogliere alcuni tra i temi ed i collegamenti possibili e qualcuno dei tanti aspetti che diventano peculiari in Internet, con un esame del quadro giuridico delle relazioni che legano operatori e utenti centrato sulle esigenze legate ai diritti della personalità. Tra questi ultimi ci interessa il diritto alla riservatezza, e conoscere meglio il fenomeno della navigazione anonima.

Queste relazioni tra operatori e utenti hanno per intermediari gli *internet provider,* il cui ruolo viene particolarmente in luce nei casi nei quali vengono messi a disposizione di terzi spazi per aprire siti e strumenti per fornire altri servizi (*hosting provider*). Nel caso di comportamenti illeciti interessa capire se ed in quale misura tali intermediari sono da ritenere responsabili e possono essere chiamati a risarcire eventuali danni. Ci interessa comunque far emergere alcuni tra i molti nodi ancora da dipanare.

2. I servizi della società dell'informazione

Le attività grazie alle quali utilizziamo la rete Internet e i servizi connessi – che a loro volta ci consentono ogni tipo di contatti ed acquisti – sono svolte da intermediari e sono considerate comprese tra i "servizi della società dell'informazione". E' l'Unione Europea a fornirne una definizione di tali servizi, con

---

avvocati (AIGA) e Conferenza dei giovani avvocati European young bar association (EYBA), Roma 9 luglio 1998. *Contra*, V. Zeno Zencovich, nel medesimo convegno.

le direttive 98/34/CE e 98/48/CE[4] cui fa rinvio la direttiva 2000/31/CE sul "commercio elettronico" (considerando n. 17 e art. 2, lett a)[5].

Si tratta di servizi prestati normalmente dietro retribuzione, a richiesta individuale di un destinatario di servizi e a distanza, per via elettronica, mediante apparecchiature elettroniche di elaborazione e di memorizzazione di dati. Vi sono compresi anche servizi non finalizzati alla stipula di contratti *on line* o non remunerati dal destinatario, ma che hanno comunque ad oggetto attività economiche, come l'offerta di informazioni o di comunicazioni commerciali in linea e la fornitura di strumenti per la ricerca, l'accesso e il reperimento di dati. Vi rientrano anche la trasmissione di informazioni mediante una rete di comunicazione, la fornitura di accesso a una rete e lo stoccaggio di informazioni fornite da un destinatario di servizi" (considerando n. 18).

Pur occupandosi soltanto di alcune questioni specifiche, la direttiva 2000/31/CE si prefigge l'obiettivo di creare un quadro giuridico inteso ad assicurare la libera circolazione di tali servizi, il cui sviluppo nello spazio senza frontiere interne è considerato uno strumento essenziale per eliminare le barriere tra i popoli europei. La direttiva contiene un riferimento particolare allo sviluppo del commercio elettronico [6], che faciliterà la crescita delle imprese, la competitività dell'industria europea e gli investimenti nell'innovazione. Purché Internet sia accessibile a tutti.

3. Linguaggio e diffidenze del cybernauta

Quello in cui si svolgono le azioni che stiamo descrivendo e vengono scambiati contenuti comunicativi è uno spazio pubblico che può essere considerato infinito. La persona vi entra rivelando la sua presenza e la sua identità, anche se attraverso strumenti della comunicazione propri di Internet. Lo scambio di segnali tra le parti si svolge, ad esempio, compilando "*form on line*", oppure selezionando opzioni sul modulo web interattivo; e ciò anche quando si aderisce a proposte di servizi. E' molto diffusa la forma del "*point and click*" (puntatura del mouse sulla zona di

[4] La *direttiva 98/34/CE* del 22 giugno 1998 del Parlamento europeo e del Consiglio prevede una procedura di informazione nel settore delle norme e della regolamentazione tecnica; la *direttiva 98/48/CE* del 20 novembre 1998 del Parlamento europeo e del Consiglio prevede una tutela dei servizi ad accesso condizionato e dei servizi di accesso condizionato.

[5] La *direttiva 2000/31/CE* dell'8 giugno 2000 del Parlamento europeo e del Consiglio ha riguardo a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("direttiva sul commercio elettronico").

[6] In Italia, alcuni autori ritengono che la locuzione " commercio telematico " risulti più adeguata.

interesse della pagina web, con una successiva digito-pressione del tasto del mouse o del corrispondente comando della tastiera), che in tal modo consente di manifestare anche la volontà di far sorgere un rapporto negoziale. A questo proposito, in Italia si è innestato un vivace dibattito - che vede protagonisti soprattutto Natalino Irti e Giorgio Oppo [7] - sulla "disumanizzazione" del contratto e l'impoverimento della sua fase di formazione, in presenza di meccanismi istantanei di adesione a condizioni poste unilateralmente. Si potrebbe facilmente obiettare, però, che i formulari non sono una novità degli ultimi anni [8]. Inoltre la navigazione in Internet facilita l'acquisizione di informazioni, e quindi probabilmente la ricerca delle offerte commerciali più convenienti.

La definizione che la direttiva 2000/31/CE dedica al "destinatario del servizio" (art. 2 e considerando n. 20) copre ogni tipo di impiego dei "servizi della società dell'informazione" da parte di persone che forniscono o cercano informazioni su reti aperte, per motivi professionali o meno. Ma il frequentatore medio della rete - in Italia e in alcuni altri paesi europei - non usa gran parte delle pur tante sue opportunità, sia per mancanza di competenze e disponibilità di tempo per acquisirle, sia per diffidenza, causata da insistenti *banners* pubblicitari o dal rischio di inconvenienti più gravi capaci di ostacolare lo stesso funzionamento del computer. Non è nemmeno molto propenso a fare acquisti e richiedere servizi, effettuare pagamenti *on line* e confidare nell'adempimento di impegni da parte di operatori che non conosce (con una eccezione nel caso di aziende e servizi molto noti, e quindi di acquisti di biglietti aerei o ferroviari e simili). Se queste preoccupazioni non esistessero, si farebbe un più intenso utilizzo dei servizi offerti nella rete anche all'interno di aziende e di amministrazioni pubbliche.

4. Esigenze di privacy, anonimato e libertà di espressione nella direttiva 2000/31/CE

Oltre a quelle descritte, altre preoccupazioni possono riguardare in modo più profondo le persone che accedono alla rete. Attraverso i particolari segnali che sono stati descritti, chi opera in Internet attraverso una connessione viene a manifestare

---

[7] OPPO G. in *Disumanizzazione del contratto*, *Riv. Dir. Civ. Vol.* I, 1998 *pag.* 528.
Secondo l'autore per gli scambi nei grandi magazzini e nei centri commerciali valgono le stesse considerazioni fatte per gli scambi telematici e le televendite. IRTI N. in " *E' vero ma…. (replica a Giorgio Oppo)*", Riv. Dir. Civ. , 1999 pag. 273.

[8] L. MANNA, *La disciplina del commercio elettronico,* Padova, 2005.

anche le proprie opinioni. Comunque manifesta la sua presenza e identità, rendendosi in qualche modo visibile e spesso rintracciabile. Viene in luce, quindi, l'interesse della persona a non essere disturbata da comportamenti anche penalmente rilevanti, o che comunque ne invadono la sfera privata (come, ad esempio e di frequente, messaggi di posta elettronica provenienti da sconosciuti).

In considerazione di questo interesse, è stabilito che ai servizi della società dell'informazione siano integralmente applicabili le direttive 95/46/CE del 24 ottobre 1995 (trattamento di dati personali e libera circolazione di tali dati) e 97/66/CE del 15 dicembre 1997 (sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni).

Sono diritti che delineano un quadro giuridico comunitario al quale occorre conformarsi in particolare per quanto riguarda le comunicazioni commerciali non richieste e il regime di responsabilità per gli intermediari. Lo specifica la direttiva 2000/31/CE sul "commercio elettronico" a proposito della protezione dei singoli in questa materia (sappiamo poi che, nel settore delle comunicazioni elettroniche, è successivamente intervenuta la direttiva 2002/58/CE).

Si dichiara anche - a conclusione del considerando n. 14 - che l'applicazione della direttiva medesima non può impedire l'utilizzazione anonima di reti aperte quali Internet [9].

Messa in luce proprio dal carattere degli scambi e dei contatti nella rete, emerge anche la centralità di un altro diritto fondamentale: nel considerando n. 9, infatti, si osserva che la libera circolazione dei servizi della società dell'informazione può riflettere specificamente il principio più generale della libertà di espressione nel diritto comunitario.

Sempre nel considerando n. 9, viene quindi ricordato l'art. 10 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (paragrafo 1), sottolineando il fatto che la tutela assicurata alla libera espressione del pensiero si estende anche alla circolazione di questi servizi. Ne consegue l'applicazione anche del paragrafo 2 dello stesso articolo, e quindi un limite alla

---

[9] Si riporta, di seguito, parte del testo del *considerando n. 14 nella direttiva 2000/31/CE*: "Dette direttive già istituiscono un quadro giuridico comunitario nel campo della protezione dei dati personali e pertanto non è necessario includere tale aspetto nella presente direttiva per assicurare il buon funzionamento del mercato interno, in particolare la libera circolazione dei dati personali tra gli Stati membri. L'applicazione della presente direttiva deve essere pienamente conforme ai principi relativi alla protezione dei dati personali, in particolare per quanto riguarda le comunicazioni commerciali non richieste e il regime di responsabilità per gli intermediari. La presente direttiva non può impedire l'utilizzazione anonima di reti aperte quali internet".

possibilità di imporre restrizioni a tale circolazione (sarebbero consentite esclusivamente le restrizioni indicate nell'art. 10, paragrafo 2, della Convenzione).

5. Diritti della persona e sicurezza in alcuni atti dell'Unione e nel decreto legislativo 70/2003

Può essere utile fare un passo indietro e ripercorrere le tracce della volontà espressa dalle istituzioni comunitarie (in vari atti) di tutelare i diritti della persona in Internet.

Da tempo sono state riconosciute e portate all'attenzione le opportunità di mercato e di lavoro offerte dalla società dell'informazione, ad esempio nell'area della vendita elettronica [10]. Ma molti atti, se pure diretti a sottolineare l'enorme importanza economica e sociale del suo sviluppo, sottolineano anche con determinazione principi ed esigenze come la trasparenza, la conoscenza, la fiducia (e quindi una necessità di tutela e di sicurezza nei confronti di quegli interessi).

La "Convenzione di Strasburgo" n. 108 del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, approvata dal Consiglio e ratificata dall'Italia con legge 21 febbraio 1989, n. 98, ha riconosciuto la necessità di conciliare i valori fondamentali del rispetto della vita privata e della libera circolazione dell'informazione tra i popoli, con una definizione di dato personale riferita ad ogni informazione relativa ad una persona fisica identificata o identificabile.

Lo scopo della Convenzione è quello di garantire sul territorio di ogni "Parte" (Stato membro) e a ogni persona fisica il rispetto dei diritti e libertà fondamentali nei casi di elaborazione automatizzata dei dati di carattere personale che la riguardano", qualunque ne sia la cittadinanza o la residenza. Per volontà dei singoli Stati membri, la Convenzione può essere applicata anche ad informazioni relative a gruppi, associazioni, fondazioni, società, cooperazioni e ad ogni altro organismo che raggruppi, direttamente e indirettamente, persone fisiche.

Più di recente, la "Risoluzione" n. 96/C376/01 del 21 novembre 1996[11], a proposito delle grandi opportunità offerte dalla **"**società dell'informazione" a beneficio dei mercati e del lavoro, ha invitato tutte le Parti a tenere conto dei suoi aspetti sociali e delle sue implicazioni per la società, e a rispettarne "la grande importanza della dimensione umana".

---

[10] In tal senso la Risoluzione n. 96/C376/01 del 21 novembre 1996 "Nuove priorità in materia di politica relativa alla società dell'informazione" (pubblicata in GUCE n. 376 del 12 dicembre 1996)

[11] Si veda la nota precedente.

La Risoluzione ravvisa anche l'esigenza di migliorare i servizi e l'accesso all'informazione pubblica, agevolando un rapido ricorso ai suoi strumenti e consolidando la fiducia del cittadino nell'uso di tali servizi, in un'ottica di tutela dei suoi diritti [12].

Interessante è anche una delle osservazioni contenute nella "Decisione del Consiglio" 30 marzo 1998, n. 98/253/CE, che approva il "Programma comunitario pluriennale per incentivare la realizzazione della società dell'informazione in Europa" [13]. In essa si sottolinea che l'avvento della società dell'informazione comporterà una riorganizzazione graduale del contenuto delle attività umane in tutti i settori, con ripercussioni intersettoriali in campi che prima erano indipendenti tra loro [14].

Nella "Risoluzione del Consiglio" 3 ottobre 2000, dedicata all'organizzazione e alla gestione di Internet, dopo aver citato la Dichiarazione congiunta UE-USA sul commercio elettronico (5 dicembre 1997), si sottolinea che è ruolo dei governi fornire un quadro giuridico coerente e prevedibile e assicurare una protezione sufficiente di obiettivi di interesse pubblico quali la vita privata, i diritti di proprietà intellettuale, la prevenzione delle frodi, la protezione dei consumatori e la sicurezza.

Abbiamo già visto, infine, che la Direttiva 2000/31/CE (commercio elettronico) contiene un riferimento alla vita privata delle persone fisiche e si occupa della protezione dei singoli nell'ambito del commercio elettronico.

Anche il diritto interno se ne occupa. Merita un accenno la relazione governativa di accompagnamento al decreto legislativo di attuazione della Direttiva sul commercio elettronico (D. lgs. n. 70 del 9 aprile 2003). Tale relazione, nell'individuare tra gli obiettivi della normativa quello di accrescere la fiducia dei consumatori nei contratti telematici, ritiene che tale fiducia "a monte deve essere riposta su meccanismi che garantiscano la sicurezza, l'affidabilità delle

---

[12] Più nello specifico, la Risoluzione pone anche in risalto la necessità di sfruttare il potenziale della società dell'informazione per valorizzare la diversità culturale e linguistica, di rendere accessibili i suoi vantaggi a ogni cittadino europeo (indipendentemente dal luogo in cui si trova o da altri motivi di esclusione) e sottolinea l'importanza che riveste la protezione dei diritti e delle libertà fondamentali (oltre che dei diritti di utenti e consumatori).

[13] L'art. 235 del Trattato istitutivo della Comunità europea (attualmente art. 308, dopo la nuova numerazione disposta dal Trattato di Amsterdam) dispone: "Quando un'azione della Comunità risulti necessaria per raggiungere, nel funzionamento del mercato comune, uno degli scopi della Comunità, senza che il presente Trattato abbia previsto i poteri d'azione a tal uopo richiesti, il Consiglio, deliberando all'unanimità su proposta della Commissione e dopo aver consultato il Parlamento europeo, prende le disposizioni del caso".

[14] Tra gli obiettivi della Commissione europea, la Risoluzione indica il compito di valutare opportunità ed ostacoli all'accesso e all'utilizzo di prodotti e servizi e di identificare misure per superarli.

comunicazioni in rete" e inoltre "la certezza dell'integrità del documento e sistemi rapidi di composizione delle controversie".

Tutte le dichiarazioni che abbiamo letto si occupano della persona non solo nella sua veste di consumatore (auspicabilmente meglio informato e più propenso ad utilizzare i servizi della rete e ad alimentare lo sviluppo del mercato). Le caratteristiche della comunicazione in Internet, infatti, e la sua capacità di propagazione hanno fatto presto mettere a fuoco il fatto che la persona, in questo particolare spazio della sua vita di relazione, può proporsi ed esporsi nei suoi aspetti ed esigenze più profondi. Di conseguenza, ne sono stati subito intuiti i rischi che possono ferire queste esigenze (anche se tutto sommato mancano approfondimenti e riflessioni di carattere sociologico e politico proporzionati all'imponenza del fenomeno e delle sue conseguenze).

Chi comunica ed entra nella dimensione pubblica della rete non dovrebbe rinunciare ad esprimersi liberamente (anzi, potrebbe e dovrebbe vedere arricchite le sue possibilità comunicative e informative). Al tempo stesso, quel "destinatario del servizio" ha diritto a vedere protetta la sua vita privata e quella dei suoi interlocutori, senza per questo essere costretto o indotto a limitare l'uso di alcuni strumenti tecnologici. Quindi l'utente deve poter confidare nel fatto che, quando utilizza tali strumenti, gli inevitabili rischi vengono sistematicamente affrontati a livello tecnologico - cercando di neutralizzarne l'uso non autorizzato - e in ogni caso a livello di sicurezza legale[15].

[15] Sunny HANDA, Mc Gill University di Montreal, relazione "*Il commercio elettronico*" al convegno cit. "*Cyber law - problemi giuridici connessi allo sviluppo di Internet".* La sicurezza legale fa riferimento alle regole della responsabilità legale che suppliscono alle lacune della sicurezza tecnologica, integrandole, stabilendo, ad esempio, chi deve sopportare il rischio della manomissione di una *password,* o attraverso l'induividuazione di clausole contrattuali che hanno l'effetto di distribuire il rischio (come avviene, ad esempio, per il calcolo di percentuali e parametri utilizzati poi per fissare commissioni, nel caso di alcuni servizi bancari)

PARTE II
IL DIRITTO ALL'IDENTITA' MINACCIATO. RIMEDIO E RICONOSCIMENTO DELLA NAVIGAZIONE ANONIMA

6. Sistemi di identificazione e profilazione dell'utente e altre minacce alla sicurezza della navigazione

Partendo dalla constatazione che le apparecchiature terminali (cellulari, terminali internet ecc.) memorizzano e trasmettono tracce delle telecomunicazioni anche all'insaputa dell'utente, si comprende perché sia nata l'esigenza di evitare di essere identificati nella rete (di cui più avanti), in modo da limitare almeno in parte le conseguenze di alcuni comportamenti.

L'acquisizione di tracce avviene in varie occasioni [16] e non sempre il loro uso rimane nei confini della liceità, né sempre l'utente viene informato ed è consapevole di quanto stia accadendo.

Molto in breve, una volta che sia stato creato un sito web, questo viene inviato ad un potente computer *(server web*); quando un utente collegato alla rete lo visita, alcune informazioni vengono conservate su *server* di custodia, in modo che i successivi utilizzatori ricevano più velocemente la pagina web (fornendosi così un'utilità complessiva agli utenti ed ottenendo anche l'effetto di ridurre il traffico sul collegamento del fornitore).

Un "*cookie*" è un contenitore di informazioni che il sito invia alla memoria interna del computer, attraverso il programma di navigazione (*browser*). Il suo uso può essere limitato alla trasmissione di numeri identificativi di sessione (generati in modo casuale dal *server*); ma un suo utilizzo sapiente può rendere anche possibile il monitoraggio - *clicktrail* – della navigazione e la ricostruzione di una "profilazione del consumatore" virtuale [17].

Anche alcuni programmi, una volta installati sul proprio computer, possono rivelare serie di informazioni relative alla navigazione. In alcuni casi, inoltre, nella pagina web possono essere presenti legami ipertestuali resi invisibili, *link* che attivano una ricerca verso un'altra parte del documento o un'altra pagina web in qualsiasi parte del mondo e all'insaputa dell'utente, o che attivano la spedizione di un messaggio di posta elettronica. E' anche possibile che messaggi e-mail

[16] Così Yves POULLET, direttore del CRID-Università de Namur, Belgio, all'incontro del Comitato consultivo del Consiglio d'Europa sulla protezione dei dati personali a Strasburgo, 28-30 giugno 2004.

[17] E. TOSI, "*La tutela dei dati personali su Internet, tra trattamento palese e occulto*"

memorizzati su un *server* possano essere verificati sulla base di determinate parole chiave, utilizzando software spia o *peepholes* (spioncini).

Esiste anche un sistema che consente di effettuare piccoli pagamenti *on line* a fronte della prestazione di un servizio. La connessione internet viene deviata a un numero telefonico a tariffazione maggiorata (evitando così all'utente di utilizzare carte di credito).

Ma in questa sequenza possono innestarsi comportamenti illeciti, talora di rilevanza penale. Vediamo come.

Il programma utilizzato per la deviazione (*Dialer*) attiva la connessione, il gestore telefonico porrà a carico dell'utente la somma dovuta al fornitore del servizio – attraverso una bolletta telefonica - e la girerà a quest'ultimo, trattenendo la quota pattuita per la propria intermediazione. Di frequente, tuttavia, si verifica che la connessione rimanga poi sistematicamente dirottata dal *Provider* originario al numero del fornitore del servizio; ciò avviene disconnettendo l'utente dal proprio *Provider*, mentre la connessione con il numero a tariffazione maggiorata viene impostata come "predefinita" (tralasciamo qui altre modalità ancora più subdole, come l'offerta di installazione di "certificati di protezione") [18].

Un fenomeno di natura diversa, che pure richiede attenzione – soprattutto se il proprio lavoro è svolto all'interno di un'istituzione pubblica o di un'azienda – è quello degli *Hacker.* Qui vi si fa solo un cenno, in quanto scopi, metodi e consapevolezza in questo caso sono diversi da quelli di coloro che attentano ai diritti della personalità e al patrimonio di un utente in quanto individuo. Nella loro espressione più genuina, questi esperti frequentatori della rete si muovono all'insegna di un progetto comune di decentramento del potere, e quindi di frammentazione e diffusione dei centri cui fanno capo informazioni e conoscenza. E' frequente che cerchino di realizzarlo penetrando nei sistemi informatici di istituzioni ritenute depositarie e protagoniste di una cultura monopolistica e conformista, con la parola d'ordine "*hands on*" (metterci le mani).

7. Sistemi di utilizzazione anonima di internet e altri strumenti e prospettive tecnologiche

Chi richiede un servizio di connessione può manifestare la volontà di utilizzare uno pseudonimo. E' anche possibile cifrare i contenuti di ciò che si trasmette all'interno di un messaggio (anche se il problema della tutela dei

[18] C. PARODI, "*Profili di rilevanza penale dei dialer*", in Diritto penale e processo 11/2003

messaggi privati viene qui affrontato incidentalmente). Tuttavia ciò non esclude la possibilità di collegare, infine, le operazioni registrate nel *log file* ad un computer e ad un numero telefonico.

Per affrontare il problema, sono stati realizzati vari sistemi. Esistono, ad esempio – e sono scaricabili e utilizzabili - programmi di cifratura della posta e di "anonimizzazione" [19].

Ma il sistema più comodo è quello di utilizzare alcuni siti che offrono un servizio di navigazione anonima, gratuitamente o a pagamento. Alcuni di essi fungono da reindirizzatori (*re-mailer*): inserendo in una casella (*form*) il proprio messaggio, questo viene automaticamente criptato e rispedito a più siti *re-mailer*. Nell'intestazione (*header*) del messaggio e-mail così trattato non compare più alcuna informazione, anche se ovviamente il percorso diviene più lungo e l'arrivo a destinazione più lento (circa 2- 4 ore e oltre).

I siti che offrono servizi di questo tipo in genere cancellano l'identificazione elettronica del mittente, mentre il loro *server* si frappone tra i siti visitati e l'utente. Quest'ultimo inserisce nell'apposito *form* l'indirizzo della pagina che intende visitare, il cui contenuto viene prelevato e reso disponibile presso di lui, mentre gli viene assegnato un IP casuale, senza registrazione dei dati.

Il sistema indicato come "*crowds*" (mescolamento nella folla) è più sofisticato e si realizza facendo rimbalzare le operazioni tra vari utenti. Alcuni sistemi creano nuovi pseudonimi ad ogni registrazione [20].

In ogni caso, il mercato offre anche altre soluzioni, e sarebbe opportuno approfondire la conoscenza delle caratteristiche dei programmi di navigazione. Alcuni *browser*, ad esempio, consentono all'utente un maggior controllo sull'ambiente e la scelta di rendersi o meno identificabile o di respingere un *cookie.*

Nell'ambito delle risposte possibili ai problemi di riservatezza e di sicurezza, è decisiva da tempo proprio la parte svolta dai progettisti di *hardware* e di *software,* con un forte impatto sulle scelte produttive e commerciali (e certamente sarà ancor più decisiva in futuro).

Un contributo importante al miglioramento dei prodotti e delle pratiche a difesa della *privacy* viene proprio dalle cosiddette *Privacy Enhancing Technologies*

---

[19] Nel 1999, in una *newsletter dell'Autorità Garante per la protezione dei dati personali*, che traduceva e riproduceva un articolo tedesco, venivano fornite indicazioni sul programma "*Pretty Good Privacy*" (P.G.P.), il primo famoso programma di anonimizzazione.

[20] Tra i più noti. Il sito "*anonymizer.com*". e in Italia il sevizio di remailing "*Antani*" (il cui nome è stato ispirato dai famosi incomprensibili dialoghi tra i protagonisti del film di Pietro Germi "Amici miei").

(PET), ovvero le certezze che le aziende - ponendosi anche in concorrenza tra loro - offrono ai propri clienti con riguardo alla sicurezza nella gestione dei loro dati e alle garanzie sulla loro cancellazione, una volta completata la transazione [21]. Sono soluzioni che possono prevedere, ad esempio, la predisposizione di programmi che, decorso un certo tempo, cancellano automaticamente le "tracce" lasciate in occasione di transazioni commerciali. Come vediamo, sono soluzioni tutte interne alle tecnologie adoperate, da considerare come elementi di una strategia più ampia e come una pre-condizione per una successiva valutazione e gestione politica dei problemi di *privacy* [22].

8. Anonimato e atti che se ne occupano, riservatezza e identità, uso delle tecnologie

In una decisione del 1995, la "Corte Suprema" negli USA sostenne che "l'identità di chi scrive non è differente da qualsiasi altra parte del contenuto di un documento che l'autore è libero di includere o escludere".

Pochi anni dopo (1997), esaminando altre esigenze, la "Commissione europea" mise in luce la necessità di sviluppare servizi di telecomunicazione alternativi in grado di garantire l'anonimato, analoghi a quelli predisposti per i pagamenti *on line*. Abbiamo poi già visto che, nell'applicare la Direttiva sul "commercio elettronico", non può essere impedita l'utilizzazione anonima di reti aperte [23].

Di recente, la "Dichiarazione sulla libertà di comunicazione in Internet" adottata dal Comitato dei Ministri del Consiglio d'Europa (28 maggio 2003) ha riconosciuto con decisione il concetto giuridico di "anonimato protetto", ricollegandolo alla tutela della libertà di espressione della quale diviene strumento [24].

Si tratta quindi di un riconoscimento esplicito.

---

[21] S. RODOTA', introduzione al convegno cit. "*Cyber law - problemi giuridici connessi allo sviluppo di Internet*".

[22] S. RODOTA', " *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione",* Laterza 2005.

[23] Cfr nota n. 8

[24] Si riproduce il testo della Dichiarazione: "Al fine di assicurare la protezione contro strumenti di sorveglianza *on line* e difendere l'espressione libera di informazioni e idee, gli Stati membri si impegnano a rispettare la volontà degli utenti internet di non rivelare la propria identità" *(Declaration on freedom of communication on the Internet, Strasburgo 28 maggio 2003, 840 th meeting of the Minsters' Deputies).*

D'altra parte quello della rintracciabilità a posteriori di chi si avvale della navigazione anonima è uno strumento ragionevole che limiterebbe il possibile conflitto con l'esigenza di indagare in caso di reati e di identificare gli autori di illeciti civili (responsabili della violazione di obblighi contrattuali o del principio del "*neminem laedere*").

In passato l'"Associazione Italiana *Internet Provider* (AAIP)" aveva già adottato un "Codice per l'autoregolamentazione dei servizi in Internet". Una tra le sue regole prevede che l'utente fornisca i propri dati identificativi e acconsenta alla registrazione (nel c.d. *log file*) delle operazioni compiute pur potendo rimanere anonimo durante l'utilizzazione di Internet. Ciò nel presupposto che le minacce alla riservatezza si realizzino solo nel momento in cui le operazioni possono essere collegate ad una persona determinata.

L'obiettivo del Codice è quello di prevenire l'utilizzo illecito o potenzialmente offensivo della rete attraverso la diffusione di una cultura della responsabilità. Pur riconoscendo un diritto di anonimato all'utente, quindi, si sostiene che questi deve essere identificabile, aderendo quindi all'idea di un "anonimato protetto" [25].

Però la regola, nella sostanza, non viene applicata, in quanto pochi *providers* adottano procedure per verificare la veridicità dei dati acquisiti.

Rispetto al tema della responsabilità, secondo il Codice occorre definire ruoli e obblighi in concreto dei soggetti di Internet. Il criterio determinante di collegamento fa perno sulla partecipazione diretta e attiva all'elaborazione di un contenuto. Solo chi ha partecipato in tali termini può essere ritenuto responsabile (non sarebbe sufficiente una collaborazione prestata in una veste tecnica, senza avere una consapevole conoscenza di quel contenuto).

Vista l'attenzione dedicata al tema da tutti gli ordinamenti giuridici che riconoscono un valore e una tutela predominante all'individuo, vale forse la pena di soffermarsi ancora sull'idea di riservatezza, anche nella sua prospettiva sociologica.

Ne abbiamo già parlato a proposito dell'incontro tra la persona e strumenti come Internet e delle modalità e dei rischi di una comunicazione attraverso la rete.

Piace ora riproporre una ricostruzione di Stefano Rodotà risalente al 1992, un periodo nel quale l'uso di queste tecnologie non era neanche così massiccio. La descrizione che l'autore fa di ciò che è "riservatezza" rinvia alla sua funzione di tutela delle scelte di vita contro il controllo pubblico e la riprovazione sociale.

---

[25] Così da tempo anche Stefano RODOTA', attuale Presidente dell'Autorità Garante per la protezione dei dati personali e, sino al 2005, del Comitato delle Autorità Garanti europee,

Lo sguardo del giurista è qui rivolto a un mondo che cambia:

"*Nuovi fatti e tendenze ci spostano sul diverso terreno delle modalità stesse di costruzione della sfera privata …. di cui l'interessato non è il solo protagonista …. Le tecnologie intervengono in quest'opera di ricostruzione, al di la delle decisioni e spesso della consapevolezza dell'interessato*".

Con pochi tratti (e con un effetto sorprendentemente incisivo) viene anche tratteggiato il modo in cui, un tempo, è emersa una esigenza e anche una possibilità di riservatezza, ricordando il ruolo essenziale che anche in questo caso hanno avuto le tecniche attraverso un'osservazione di Lewis Humford:

"*Il primo mutamento radicale, destinato a infrangere la forma della casa di abitazione medioevale, fu lo sviluppo del senso di intimità …. durante il sonno, durante i pasti; intimità nel rituale religioso e sociale; finalmente, intimità nel pensiero*".

Aggiunge Rodotà che la nascita e la percezione di questo bisogno può essere ricondotta al disgregarsi della società feudale, in cui l'isolamento era privilegio di pochissimi eletti.

Rodotà sottolinea che più tardi la nozione riguarderà l'insieme delle attività e delle situazioni di una persona che hanno un potenziale di "comunicazione" verbale e non verbale, e che si possono tradurre in informazione. Privato ormai vuole dire "personale", senza che questo comporti necessariamente esigenze di segretezza [26].

Dopo aver messo a fuoco questo patrimonio e datone oramai per scontato il valore, torniamo alla nostra analisi attuale sull'uso delle tecnologie e di Internet e alle nostre preoccupazioni.

Oltre a voler difendere la nostra sfera strettamente privata, può allarmarci il fatto che le informazioni raccolte su di noi vengano a comporre una identità che prende corpo in un luogo particolare (ed è la novità legata alla natura virtuale dell'informazione prodotta e circolante in Internet).

Questa identità, infatti, potrebbe venire costruita in modo da non coincidere con ciò che siamo, come in un mosaico della nostra immagine in cui vengano a mancare pezzi fondamentali, o alcune parti risultino alterate. In questo senso, quello che viene indicato come un "diritto alla identità" si pone a metà strada tra la riservatezza e la libertà di espressione, come diritto a non vedere alterata la verità

[26] S. RODOTA', *Repertorio di fine secolo*, Laterza, 1992, con considerazioni recentemente sviluppate nella cit. op. *Tecnopolitica*.

della propria vicenda umana e storica e dunque a non vedersi attribuito un pensiero che non è "proprio" [27].

Quindi è da considerare normale – e non con sospetto - la preoccupazione di chi voglia evitare di navigare nella rete e di utilizzarne i servizi fornendo informazioni collegabili al proprio nome e alla propria persona. Queste informazioni su di noi e sulle nostre opinioni permangono infatti al di fuori del nostro controllo, e lontano e anche contro la volontà e possibilità di mutamento del nostro pensiero e del modo di esprimere la nostra persona.

Più in generale e incidentalmente, in Italia la delicatezza del tema è stata colta anche dal legislatore penale. La legge n. 547 del 23 dicembre 1993, infatti, nell'introdurre nuove figure di reato, ha equiparato il sistema informatico a quelle che erano le relazioni di luogo tradizionali (le abitazioni e i luoghi di dimora privata), e quindi una intrusione informatica viene considerata una violazione di domicilio [28].

[27] In tal senso, già Cass. 3199/1960 del 7 dicembre 1960, che pure negava protezione al diritto alla riservatezza.

[28] P. GALDIERI, relazione " *La tutela penale della nuova frontiera elettronicd*' al convegno citato *Cyber law - problemi giuridici connessi allo sviluppo di Internet* '". La legge citata inserisce gli articoli 615-*ter* "accesso abusivo ad un sistema informatico o telematico", 615-*quater* "detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici" e 615 -*quinques* "diffusione di programmi diretti a danneggiare o interrompere un sistema informatico" nella parte del codice che si occupa della tutela del domicilio (II libro del codice penale, Titolo XII, capo terzo, sezione quarta).

PARTE III
OBBLIGHI E RESPONSABILITA VERSO GLI UTENTI. RUOLO DELLE IMPRESE E DEGLI ORGANI PUBBLICI

9. Le diverse categorie di prestatori di servizi in Internet

Dopo essere entrati nel vivo dei fenomeni, ritorniamo ad interessarci del quadro giuridico delle relazioni che legano operatori e utenti in Internet. Il ruolo del fornitore di servizi Internet ci interessa per capirne gli obblighi a fronte delle esigenze di tutela dei diritti e interessi di cui abbiamo parlato, e il modo in cui tali obblighi si atteggiano.

Di conseguenza, nel caso di comportamenti illeciti di terzi, interessa capire in quali casi anche il *provider* possa essere ritenuto responsabile e possa essere chiamato a risarcire eventuali danni, o se comunque debba almeno garantire l'identificabilità dei potenziali autori di illeciti.

La genericità del termine è stata superata dalla direttiva sul "commercio elettronico" (per questa parte, pedissequamente trasposta nel decreto legislativo n. 70/2003), che ha individuato 3 categorie di providers rispetto al trattamento delle informazioni fornite da un destinatario di un "servizio della società dell'informazione". Sintetizzando, possono essere svolti servizi:

a) di semplice trasporto su una rete di comunicazioni, consentendo, ad esempio, l'accesso alla rete ("*mere conduit*", art 14);
b) di memorizzazione temporanea, allo scopo di rendere più efficace il successivo inoltro ad altri destinatari ("*caching*", art. 15);
c) di vera e propria memorizzazione, con l'offerta di un servizio commerciale di conservazione delle informazioni, come la pubblicazione di messaggi nell'ambito di newsgroup o l'offerta di spazi per aprire siti o *blog* ("*hosting*", art. 16).

Di seguito si riporta il testo degli articoli 14, 15 e 16 del D. Lgs. n. 70/2003:

14. Responsabilità nell'attività di semplice trasporto - Mere conduit.

1. Nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione, il prestatore non è responsabile delle informazioni trasmesse a condizione che:

a) non dia origine alla trasmissione;
b) non selezioni il destinatario della trasmissione;
c) non selezioni né modifichi le informazioni trasmesse.

2. Le attività di trasmissione e di fornitura di accesso di cui al comma 1 includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo.

3. L'autorità giudiziaria o quella amministrativa, avente funzioni di vigilanza, può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 2, impedisca o ponga fine alle violazioni commesse.

15. Responsabilità nell'attività di memorizzazione temporanea - caching.

1. Nella prestazione di un servizio della società dell'informazione, consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che:

a) non modifichi le informazioni;
b) si conformi alle condizioni di accesso alle informazioni;
c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore;
d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni;
e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione.

2. L'autorità giudiziaria o quella amministrativa aventi funzioni di vigilanza può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse.

16. Responsabilità nell'attività di memorizzazione di informazioni - hosting.

1. Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:

a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione;
b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

2. Le disposizioni di cui al comma 1 non si applicano se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore.

3. L'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse.

Sono servizi differenti che tuttavia possono venire svolti anche dal medesimo *provider*, o anche offerti contemporaneamente allo stesso utente o abbonato. Per saperlo bisogna esaminare i singoli accordi conclusi tra le parti.

Qui interessa soprattutto la terza ipotesi (*hosting*). Attraverso gli spazi e strumenti messi a disposizione in questo genere di servizi un soggetto potrebbe adottare comportamenti di concorrenza sleale (utilizzando ad esempio marchi altrui), violare diritti di proprietà intellettuale (vendendo opere), adottare comportamenti lesivi dell'altrui riservatezza e di altri diritti della personalità (trasmettendo messaggi pubblicitari indesiderati o carpendo informazioni) o arrecare comunque un pregiudizio. Potrebbe addirittura commettere reati (come la diffusione di messaggi ritenuti diffamatori, oppure l'organizzazione di truffe).

Per orientarsi e a fini limitati, può essere tenuta presente la distinzione fatta da alcuni autori tra illeciti "di Internet" (violazioni commesse dai soggetti che gestiscono la rete), illeciti "contro Internet" (di utenti a danno della Rete e dei suoi operatori) e "per mezzo di Internet". Tra gli illeciti per mezzo di Internet sono compresi gli illeciti contro i diritti della personalità.

10. Posizione e obblighi dei prestatori di servizi *hosting*

Se è vero che un soggetto mette a disposizione gli strumenti senza i quali la condotta non avrebbe potuto realizzarsi, si pone un problema di riconducibilità in capo allo stesso della condotta illecita dell'utilizzatore (e di imputazione di obblighi di risarcimento).

Naturalmente *nulla quaestio* nei casi in cui, oltre a servizi di *hosting*, il fornitore sia anche un *content provider* (fornitore di contenuti), in quanto sarà responsabile civilmente per fatto proprio ove vengano accertati illeciti compiuti in tale veste.

Parte della dottrina ha oscillato tra l'individuazione di una responsabilità di tipo oggettivo (basata su una possibile redistribuzione dei danni in ragione della natura imprenditoriale degli operatori), di una responsabilità analoga a quella dell'editore della stampa periodica (teoria sostenuta soprattutto in passato), e di una responsabilità para-oggettiva, basata su un criterio di collegamento quale quello dettato dall'art. 2050 del codice civile per tutti i casi di svolgimento di attività pericolose (ad esempio, per intendersi, in caso di guida di un veicolo a motore).

Quando un'attività viene considerata pericolosa, una delle conseguenze più rilevanti consiste nell'inversione dell'onere della prova rispetto alla normalità dei casi, con l'autore della condotta che deve provare di aver adottato un comportamento idoneo a prevenire il danno che invece si sia verificato. L'idoneità

viene valutata alla stregua delle norme e delle regole tecniche dettate per la materia o per la tipologia del caso.

Chi propende per questa figura di responsabilità non ritiene, in genere, che la pericolosità risieda nella natura dell'attività, ma piuttosto negli obblighi informativi nei confronti dell'autore - che deve essere stato messo al corrente delle responsabilità in cui può incorrere - e in relazione alla responsabilità che ci si assume di garantire l'anonimato [29].

Anche la giurisprudenza – che in materia è piuttosto limitata - si è occupata della responsabilità dell'*hosting provider.*

Tralasciando qui le sentenze in materia penale, il dato di massima è che le decisioni hanno quasi sempre rigettato ipotesi di imputazione oggettiva, prestando invece attenzione alle concrete modalità del servizio prestato [30].

Tralasciamo anche quella fase in cui la giurisprudenza civile – avallata più tardi dalla legge che aveva ampliato oltre misura il concetto di prodotto editoriale (legge sull'editoria n. 62/2001) – qualche volta aveva considerato responsabile il soggetto che aveva messo a disposizione spazi ospitanti contenuti lesivi, ritenendone la posizione equiparabile a quella dell'editore nella stampa periodica [31].

Tornando quindi ad esaminare la normativa, riscontriamo subito l'affermazione di principio più rilevante, che è quella che chiarisce che non esiste un obbligo generale di sorveglianza sulle informazioni memorizzate, contenuta nella direttiva 2000/31/CE (art. 15, comma 1) e nel decreto legislativo di recepimento 70/2003 (art. 17, comma 1) [32].

L'obiettivo era quello di trovare un equilibrio tra due esigenze in antitesi: non paralizzare le nuove attività ed evitare la totale estraneità degli intermediari.

---

[29] DI CIOMMO, *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, 2003.

[30] In precedenza il Tribunale di Roma, in un caso di diffamazione, non aveva ritenuto possibile una assimilazione al regime delle testate giornalistiche, poiché solo l'esistenza di un controllo da parte di un moderatore avrebbe potuto fondare una responsabilità.

[31] L'interpretazione è stata definitivamente superata grazie all'art. 7, comma 3, del d.lgs. 70/2003, che chiarisce che la registrazione della testata telematica è obbligatoria solo se ci si avvale delle provvidenze previste dalla legge 62/2001.

[32] Si riporta di seguito il testo dell'art. 17, comma 1, del d.lgs. 70/2003. Art. 17 (Assenza dell'obbligo generale di sorveglianza). *1. Nella prestazione dei servizi di cui agli articoli 14, 15 e 16, il prestatore non e' assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.*

La normativa - con l'art. 16, comma 1 - lo ha perseguito reinserendo l'elemento soggettivo della colpa al centro delle valutazioni da operare per poter collegare una responsabilità alla fattispecie concreta[33]**.** Si è fatto ricorso a ipotesi di colpa tipizzata (le situazioni che nella disposizione vengono costruite apparentemente come esimenti)[34]**.** Le ragioni della scelta sono comprensibili. Sarebbe tecnicamente impossibile, infatti - oltre che dispendioso – realizzare un controllo di tutte le attività e di tutti i contenuti che i servizi *hosting* consentono di produrre.

Leggendo il citato art. 16, comma 1, e ponendolo a confronto con l'articolo 17 (non riferito al solo *hosting,* ma comune a tutte le categorie di servizi disciplinate nei precedenti articoli 14, 15 e 16), pare che il comportamento al quale il *provider* è tenuto abbia ad oggetto solo l'informazione da fornire all'Autorità competente, amministrativa o giurisdizionale (e non un intervento di rimozione di messaggi o di interruzione di un servizio dell'abbonato o utente)[35].

Questa informazione, letta nell'art. 17 (come dicevamo riferito a tutte le categorie di servizi), dovrebbe riguardare l'esistenza di presunte attività illecite (comma 2) o pregiudizievoli per un terzo (comma 3) compiute da un destinatario del servizio offerto dal *provider,* e sembra riferirsi a una fattispecie differente da quella prevista dall'art. 16 per i servizi *hosting* [36].

---

[33] In base all'art. 16, comma 1, lett. a) del D. Lgs. 70/2003 il prestatore del servizio è responsabile se è "effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita" e, per quanto attiene ad azioni risarcitorie, sia al corrente di fatti o circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione". In base alla successiva lett. b), è responsabile se "non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti", non agisca immediatamente per rimuovere le informazioni o disabilitare l'accesso".

[34] In tal senso anche BUGIOLACCHI, *La responsabilità dell'host provider alla luce del d.lgs. 70/2003: esegesi di una disciplina dimezzata,* in "Responsabilità civile e previdenza", Milano, fasc. 1/2005.

[35] Non così G. CASSANO, *Diritto dell'Internet, il sistema di tutele della persona*, Giuffrè, 2005. L'autore ritiene che le due ipotesi produttive di responsabilità previste dall'art. 16 siano autonome.

[36] Si riporta di seguito il testo dell'art. 17 del D.Lgs. 70/2003, commi 1 e 2 (per il testo del comma 1, si veda la nota 32). *2. Fatte salve le disposizioni di cui agli articoli 14, 15 e 16, il prestatore e' comunque tenuto: a) ad informare senza indugio l'autorita' giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attivita' o informazioni illecite riguardanti un suo destinatario del servizio della societa' dell'informazione; b) a fornire senza indugio, a richiesta delle autorita' competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attivita' illecite. 3. Il prestatore e' civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorita' giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza*

Tra l'altro nell'art. 17 si terrebbe conto della vigenza di un rapporto contrattuale, collegandovi un dovere di informazione riferito ai dati identificativi del proprio destinatario del servizio (lett. b) del secondo comma). In conclusione ne emerge un obbligo di acquisire preventivamente i dati, per poterli mettere a disposizione all'occorrenza (ovvero in seguito alla denuncia di quel comportamento pregiudizievole) [37].

Accennavamo prima a un intervento diretto del *provider,* esigibile però solo in presenza di una "comunicazione" dell'Autorità competente (art. 16, comma 1, lett. b) o di un "provvedimento" amministrativo o giurisdizionale. Lo si evince dall'art. 17, comma 3, prima parte, e dall'art. 16, comma 3. Per inciso, quest'ultima norma – come le parallele disposizioni riferite ai servizi *"mere conduit"* e "*caching*" - dispone che il giudice che sia stato adito utilizzando il procedimento d'urgenza ex art. 700 cod. proc. civ. possa esigere un intervento che impedisca o ponga fine a comportamenti lesivi direttamente dal *provider* (e non solo dall'autore diretto). La disposizione sembrerebbe superflua. Ma probabilmente la sua formulazione è una risposta alle perplessità nutrite in passato circa la possibilità di coinvolgere un soggetto estraneo al procedimento cautelare (perplessità peraltro giustificate)[38].

Pensando a un'applicazione concreta alla luce delle norme, secondo alcuni autori vi sarebbe un obbligo di informazione a carico del fornitore di *hosting* nel caso di un fenomeno come quello dei *dialer* (dei cui inconvenienti abbiamo parlato)*:* una sua eventuale presenza sarebbe infatti talmente palese da far ritenere che il fornitore "non possa non sapere" che sui propri server alcuni clienti lo utilizzano. Trattandosi di una situazione potenzialmente lesiva per il proprio cliente, il fornitore dovrebbe quindi portarla a conoscenza dell'Autorità[39].

11. Un equilibrio tra interessi affidato alle imprese

Anche dopo l'intervento del decreto legislativo 70/2003, rimangono molte zone d'ombra con cui fare i conti. La normativa di recepimento interno non precisa neanche quali sono le Autorità competenti, alle quali la direttiva 2000/31/CE fa

---

del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorita' competente.

[37] L'obbligo è già previsto dal citato Codice di autoregolamentazione dell'AIIP (cfr. paragrafo 9).

[38] Per un esempio, si legga P. COSTANZO, *nota alla sentenza del Trib. Di Teramo 11 dicembre 1997*, in "Diritto dell'informazione e dell'informatica", fasc. 2/1998.

[39] C. PARODI, "*Profili di rilevanza penale dei dialer*" riv. cit., condividendo la posizione espressa da A. MONTI, *La catena delle responsabilità nella diffusione dei dialer*, in www.interlex, 2003.

ovviamente un semplice cenno, non dovendo incidere oltre nell'organizzazione interna degli Stati membri.

Rispetto ai profili di carattere civilistico e nella pratica negoziale, si può porre rimedio a quelle zone d'ombra prevedendo apposite clausole nei contratti che chiariscano le obbligazioni reciproche tra *provider* e abbonato o utente. Rispetto al dovere di informare, si può ritenere che in caso di segnalazione (non da parte di un'Autorità, ma dell'interessato) il *provider* abbia l'obbligo di attivarsi subito, per effettuare tutte le verifiche che servono a mettere l'Autorità competente in grado di decidere.

Manca ancora, evidentemente, un quadro di riferimento di compiti e procedure sufficientemente chiaro, soprattutto in ambito amministrativo. Il segno complessivo della disciplina è comunque quello di assegnare al *provider* un ruolo di cooperazione con le Autorità.

Forse converrebbe agevolare la possibilità di rivolgersi direttamente alle Autorità competenti, pur se opportuno che, in via normale, la richiesta della persona che si ritenga lesa pervenga per il tramite di un soggetto qualificato come il fornitore dei servizi. Per ora è facile prevedere che i più avveduti si rivolgeranno all'Autorità amministrativa, e in caso di urgenza cercheranno anche di ottenere un intervento immediato del *provider.*

Nulla esclude, infatti, che quest'ultimo agisca in maniera autonoma (nella pratica negoziale generalmente ci si riserva tale possibilità, ad evitare di rimanere esposti alle conseguenze di una violazione di obblighi contrattuali). Ma un sistema che incentivi soluzioni di questo genere in realtà non è stato costruito.

Il dibattito degli anni '90 aveva messo in luce i rischi che avrebbe comportato l'introduzione di un fattore di sostanziale arbitrio, rimesso solo alla valutazione degli imprenditori. Questi ultimi possono non disporre delle risorse necessarie per tutelare un ragionevole equilibrio di interessi tra parti in conflitto, e soprattutto non avere l'interesse a salvaguardare esigenze di libertà. Questo genere di perplessità e il pericolo di scelte casuali o opportunistiche hanno indotto le associazioni di *providers* a elaborare strumenti alternativi di risoluzione delle controversie per demandare la decisione a organi terzi, anche per bypassare alcuni conflitti di legge e di giurisdizione [40].

[40] M. DOTTI, relazione su "la soluzione delle controversie su Internet" al cit. convegno "Ciber law – *problemi giuridici connessi allo sviluppo di Internet*".

12. Rischi per la libertà di espressione. Tra responsabilità dei *providers* e azioni giudiziarie di risarcimento

Grazie ad alcuni servizi di Internet forse oggi è più facile manifestare il proprio pensiero e conoscere quello degli altri, e quindi formare un pensiero critico. Ciò anche con riferimento alle scelte di consumo. A tale proposito e per quanto riguarda la normativa italiana, merita un cenno la già citata relazione governativa di accompagnamento al decreto legislativo n. 70/2003, decreto che si proporrebbe "di sviluppare un'economia basata sulla conoscenza" pervenendo, attraverso regole chiare e trasparenti, a costi di produzione minori e a una migliore scelta e qualità dei prodotti.

Da tempo si parla anche di un nuovo diritto di libertà informatica della persona, una libertà attiva di vigilare, trasmettere e ricevere informazioni [41].

Conviene ricordare anche che la direttiva 2000/31/CE sul commercio elettronico, pur a proposito di casi nei quali sussiste una responsabilità del *provider* in presenza di attività illecite, afferma che la rimozione delle informazioni o la disabilitazione dell'accesso devono essere effettuate nel rispetto del principio della libertà di espressione (considerando n. 46), che è tutelata dall'art. 10, par. 1, della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

Sulla linea delle riflessioni fatte circa l'inopportunità che sia il *provider* a decidere direttamente la rimozione di un contenuto, è storia molto vicina a noi – nel diverso ma contiguo ambito di attività del servizio pubblico radiotelevisivo e della stampa tradizionale – quella che vede affermarsi una diversa finalità delle denunce per diffamazione e delle azioni giudiziarie in sede civile. Per il timore che il denunciante avanzi esose richieste di risarcimento di danni, infatti, diventa possibile dare facile agio all'affermarsi di poteri forti, impedendo o censurando alcune attività e la manifestazione di alcune opinioni. Ciò in assenza, in generale, di contrapposizioni dialettiche di sostanza, destinate a lasciare il passo ad argomentazioni divenute, a quel punto, esclusivamente di carattere economico. Ove anzi le richieste di risarcimento dovessero assumere sempre più finalità intimidatorie, sarebbero sempre più spropositate, paralizzando piccoli imprenditori o – fuori dell'ambito delle attività di natura strettamente commerciale – associazioni o singoli, interessati a comunicare iniziative e prese di posizione su fatti di attualità.

---

[41] Così V. FROSINI, introduzione al cit. convegno "*Ciber law – problemi giuridici connessi allo sviluppo di Internet*". Tale diritto si sostanzierebbe nell'esercizio di "un controllo sulla gestione che altri compie di fatti informatici concernenti la vita intima, la riservatezza personale e la dignità umana di un soggetto giuridico".

Si pone quindi un problema di parità sostanziale nell'accesso agli spazi sociali e alle attività economiche e politiche. C'è il rischio che i centri di assunzione delle decisioni destinate a incidere su tali interessi vengano ad essere svincolati dalla rappresentanza, e soprattutto anche estranei alla dimensione nella quale trovano valore e possibilità di espressione principi come la tutela delle minoranze e di soggetti deboli.

Un po' più lontana da noi geograficamente – ma anch'essa storia di questi giorni – la vicenda di persone addirittura inquisite o imprigionate per aver espresso opinioni in dissenso rispetto alle posizioni del governo del proprio paese, opinioni considerate e punite come reati. Ciò in virtù di accordi in base ai quali i *providers* si impegnano a fornire informazioni sui contenuti e sulla provenienza dei messaggi (è accaduto recentemente in Cina, dove la trasmissione all'estero di una notizia da parte di un giornalista è stata considerata una minaccia per la sicurezza, e in Tunisia, in occasione di alcune ricerche effettuate in rete di studenti universitari).

E' in sintonia con queste considerazioni il modo in cui Stefano Rodotà, prendendo le mosse da una riflessione sull'esistenza di un deficit di democrazia e sull'utilità di individuare alcuni suoi caratteri tipici, collega il tema della partecipazione alla democrazia, "*che si svela come un processo, mai compiuto e sempre più esigente …… di inclusione di persone e situazioni nella logica e nelle regole democratiche*". Nei regimi democratici, quindi, si rinverrebbe una concreta attitudine a produrre inclusione. E il processo democratico si legherebbe all'informazione, che ne costituisce una delle "pre-condizioni": si deve aver riguardo, quindi, alla quantità di "informazioni rilevanti" che circolano, a chi le produce, al grado di accesso diretto dei cittadini e ai mezzi per vagliarle criticamente e diffonderle [42].

Più recentemente l'autore ha messo in luce il fatto che il ricorso all'anonimato può essere funzionale alla partecipazione svolgendo una funzione di tutela dell'individuo e della sua identità, pur mettendo all'erta rispetto all'illusione romantica di una totale mancanza di regole, che non metterebbe al riparo da degenerazioni e dall'influenza di preponderanti interessi economici.

[42] S. RODOTA', op.cit. *Repertorio di fine secolo*, con considerazioni sviluppate in recenti interventi sulla stampa

13. La protezione dei dati personali *on line*

Per stabilire la disciplina applicabile nel trattamento *on line* dei dati personali, il criterio di collegamento è quello classico del diritto internazionale, e quindi il legame fisico tra l'azione compiuta e il sistema giuridico. Si applica, quindi, la normativa del territorio dell'Unione Europea in cui si trovano gli strumenti utilizzati per il trattamento (automatizzato e non), anche nel caso in cui il "luogo di stabilimento" del titolare del trattamento sia altrove.

Nel caso di violazioni che ledono il diritto alla tutela dei dati personali (ad esempio rispetto ai dati forniti direttamente al fornitore del servizio), il criterio di collegamento per individuare la responsabilità civile è fornito dall'art. 2050, con un'inversione dell'onere della prova a carico di chi, organizzando l'attività considerata pericolosa, abbia arrecato danni o non applichi misure di sicurezza adeguate [43].

Il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta le misure di sicurezza che riguardano la rete insieme al fornitore della rete pubblica di comunicazione. Il primo fornitore deve poi informare gli abbonati (e in tutte le occasioni in cui è possibile gli utenti) circa l'esistenza di particolari rischi di violazione della sicurezza della rete, anche nei casi in cui non sia tenuto ad intervenire [44].

Il codice per la protezione dei dati personali disciplina in maniera specifica le comunicazioni elettroniche (articoli da 121 a 134), introducendo il divieto di accedere attraverso una rete di comunicazioni elettroniche a informazioni archiviate nell'apparecchio terminale di un abbonato o utente, al fini di archiviare informazioni o monitorare operazioni.

Per i contenuti comunicativi di messaggeria privata o di messaggeria pubblica (questi ultimi sono quelli immessi nelle aree pubbliche del *web* e liberamente consultabili), è titolare del trattamento il soggetto che crea ed emana tali contenuti. Invece, *il provider* che appresta il mezzo tecnico mediante il quale avviene la trasmissione (o memorizzazione) dei dati - e quindi non fornisce i contenuti ma il servizio utilizzato - è titolare del trattamento quando raccoglie i dati che i propri clienti "disseminano" durante la navigazione. Tratta quindi - e deve proteggere - le

[43] In caso di omissione di misure minime di sicurezza sono previste anche sanzioni penali

[44] Così l'art. 32 del D.Lgs. n. 196 del 30 giugno 2003, "Codice in materia di protezione dei dati personali"

tracce contenute nel registro della navigazione Internet (*i log files*) o altre tracce informatiche (per lo più dati identificativi dell'elaboratore dal quale provengono le informazioni inviate) [45].

14. La tutela dei dati personali in Italia: la normativa non è comunemente percepita come tutela di un diritto di libertà

Per concludere sull'anonimato, ci sembra di dover aggiungere che quando le vicende e i contesti di riferimento sono quelli di paesi a democrazia limitata (pensando ai casi e agli episodi prima citati, accaduti in Cina e in Tunisia), si riapre il capitolo che pone attenzione all'opportunità di rimanere del tutto anonimi, non identificabili neanche a posteriori, capitolo che a questo punto non possiamo che lasciare aperto.

Vogliamo anche riferire, infine, qualche impressione che è possibile verificare osservando il modo in cui si avvicina alla normativa del Codice per la protezione dei dati personali la maggior parte dei non addetti ai lavori (dei non esperti, tenuti tuttavia a conoscerlo e applicarlo).

Se si pensa anche al tenore dei primi atti internazionali che si sono occupati di protezione dei dati personali, bisogna riconoscere che, da quando la definizione di "dato personale" è stata riferita anche agli enti (e non elusivamente alle persone fisiche), è diminuita la percezione della portata ideale della normativa. Lo si può certamente almeno sostenere per quanto riguarda l'Italia.

La correttezza della definizione è fuori di dubbio, né si può disconoscere che le norme in effetti affermano alcuni principi con determinazione e impongono i comportamenti conseguenti. Piuttosto, se la preoccupazione era quella di ovviare alla possibile ripetizione di concetti e regole che risultano comuni anche ai dati non riferiti agli individui (o meglio, pur sempre indirettamente riferiti agli individui, ma attraverso gli enti), forse poteva essere trovato un espediente per semplificare e sistemare la materia che non ne diluisse i contenuti e l'incisività.

Nonostante la sua grande importanza, purtroppo questa normativa non attrae le persone più sensibili al tema dei diritti e delle libertà. E' un dato di fatto doloroso per chi ha a cuore l'affermarsi di effettivi spazi di libertà e di dignità per l'individuo e le piccole comunità a fronte di interlocutori o apparati che rischiano di soffocarli.

[45] G.CASSANO, "*Diritto dell'Internet. Il sistema di tutele della persona*", Giuffrè, 2005

La normativa non attrae certamente al primo incontro, e non prima di avere avuto l'occasione di entrare in contatto con esperienze, riflessioni e interpretazioni capaci di aprire una prospettiva più ampia.

Altri soggetti costretti a fare i conti la normativa (piccoli operatori economici, dipendenti di aziende o di amministrazioni pubbliche, professionisti) - e che incamerano e conservano quotidianamente grandi quantità di informazioni su clienti, fornitori, cittadini e pazienti - non sono inclini ad ampliare l'orizzonte delle loro preoccupazioni al di là della necessità di adempiere a un obbligo pericolosamente sanzionato. Il loro approccio normalmente non ha nulla a che vedere con la consapevolezza con la quale - per fortuna – vengono invece percepite e rispettate altre regole nel campo dei diritti individuali.