MIRIAM VIGGIANO

« NAVIGAZIONE » IN INTERNET E ACQUISIZIONE OCCULTA DI DATI PERSONALI

SOMMARIO: 1. L'originario riconoscimento del *right to privacy* nell'ordinamento americano nella sua accezione di tutela dell'inviolabilità della persona e della sua libertà di scelta — 2. *Privacy* e riservatezza: un rapporto di genere a specie. Il fondamento costituzionale del diritto alla riservatezza nell'ordinamento italiano. — 3. L'affermazione delle nuove tecnologie informatiche e delle banche dati telematiche: il problema della determinazione del contenuto del diritto alla riservatezza in rapporto con altri interessi costituzionalmente rilevanti. — 4. Internet come nuovo mezzo di raccolta e diffusione delle informazioni degli utenti. I beni giuridici informatici e tutela del cd. ''domicilio informatico''. — 5. Il valore economico delle informazioni registrate via Internet e le modalità tecniche per creare un esatto profilo sociale dell'utente telematico. — 6. La protezione dei dati personali fra diritto interno e diritto comunitario. La normativa applicabile ad Internet in attesa dell'approvazione del codice di deontologia dei fornitori di comunicazioni e informazioni. — 7. L'estensione della normativa vigente. La distinzione fra trattamento dei dati « a raccolta palese » ed « a raccolta occulta ». — 8. Dati di traffico, file di *log* e tutela della riservatezza. — 8.1. Il problema della conservazione per fini di sicurezza dei dati relativi alle comunicazioni trasmesse attraverso la rete Internet. — 8.2. La sospensione delle disposizioni sulla cancellazione dei dati riguardanti il traffico delle comunicazioni elettroniche e la modifica dell'art. 132 del codice della *privacy*. — 9. Altre tecniche di raccolta invisibile dei dati: *browsing chattering*, *cookies*, programmi *spyware*. Il ''diritto all'informazione'' del navigatore telematico. — 10. Il problema dell'a-territorialità del fenomeno Internet e le conseguenze sulla tutela della riservatezza degli utenti. La necessità di avviare un dibattito di dimensione 'globale'.

1. L'originario riconoscimento del *right to privacy* nell'ordinamento americano nella sua accezione di tutela dell'inviolabilità della persona e della sua libertà di scelta.

La tutela di ciò che è privato, ovvero di ciò che è di esclusiva pertinenza del singolo individuo e della dimensione strettamente personale o familiare

* Il presente lavoro costituisce la rielaborazione di una parte della tesi di dottorato dal titolo « Informazione e nuove tecnologie: come la diffusione di Internet trasforma l'applicazione dei principi costituzionali » che ha ricevuto il « Premio Vittorio Frosini per l'informazione giuridica e il diritto dell'informatica » nella edizione del 2006.

delle sue attività — con esclusione dell'ingerenza di estranei non autorizzati — è quello che costituisce il cuore del *right to privacy*.

Si tratta di un diritto di amplissima portata la cui prima elaborazione dottrinale, contenuta nel noto saggio di Warren e Brandeis, si è avuta negli Stati Uniti che lo ha ricondotto nell'alveo dei diritti della personalità a protezione dell'immunità e dell'inviolabilità della persona[1]. Si deve, infatti, a questi autori l'avere sviluppato la tesi dell'esistenza di un autonomo diritto alla *privacy* slegato sia dalla proprietà privata che dalla disciplina dell'ingiuria e della diffamazione — con cui vi sarebbe stata una rassomiglianza solo superficiale[2] — e diretto a proteggere sentimenti e pensieri connessi con la sfera personale/emotiva del singolo facendo assumere rilevanza giuridica alla « sofferenza mentale » derivante dalla comunicazione al pubblico di qualcosa di proprio senza consenso[3].

Nonostante la novità della dottrina richiamata e l'eco realizzatosi in letteratura[4], i successivi richiami della giurisprudenza americana hanno continuato ad ancorare il relativo diritto alla proprietà privata o alla reputazione[5]; mentre negli anni Sessanta si è tentato di 'smontarlo' cercando di dimostrare l'inesistenza di un'autonoma figura giuridica e la sua distinzione in quattro diversi illeciti civili[6] derivanti: dall'invasione nella « solitudine » o negli affari del singolo, dalla diffusione di fatti imbarazzanti riguardanti la vita privata, dal porre una persona in cattiva luce agli occhi

---

[1] S.D. Warren-L.D. Brendeis, *The right to privacy*, in *Harvard Law Review*, vol. IV, n. 5, 1890, 207 in cui espressamente si definisce « [...] *the right to privacy, as a part of the more general right to the immunity of the person, — the right to one's personality* ».

[2] È la traduzione delle parole utilizzate nel saggio di S.D. Warren-L.D. Brendeis, *The right to privacy*, cit., 197.

[3] In tal senso, S.D. Warren-L.D. Brendeis, *The right to privacy*, cit., 197 che precisano come la diffamazione « *deals only with damage to reputation, with the injury done to the individual in his external relations to the community, by lowering him in the estimation of his fellows* ». Essa non ha alcuna attinenza con la stima che il soggetto ha di se stesso ed i suoi sentimenti non costituiscono un elemento essenziale dell'azionabilità del diritto. Come è dalla dottrina citata riassunto: « *In short, the wrongs and correlative rights recognized by the law of slander and libel are in their nature material rather than spiritual* » (p. 197). Sul punto cfr. anche le considerazioni di A. Baldassarre, *Privacy e costituzione. L'esperienza statunitense* Roma, 1974, 42 ss. che evidenzia anche come il *right to privacy*, nel pensiero di Warren e Brendeis, « si distingua tanto dal diritto all'onore quanto dalla proprietà privata, adducendo la spiegazione che, da un lato, il danno causato alla sua violazione si commisura, non già alla diminuzione della stima nei propri consociati, bensì nella propria sofferenza mentale e, dall'altro, che il fondamento che lo giustifica non è quello ''materiale'' della proprietà, bensì quello ''spirituale'' dell'inviolata personalità » (in particolare p. 300).

[4] Pochi sarebbero stati gli autori non concordi con la tesi descritta; ma sul punto si rinvia alla bibliografia citata da W.L. Prosser, *Privacy*, in *California Law Review*, vol. 48, n. 3, 1960, 384 in nota 7.

[5] A. Baldassarre, *Privacy e Costituzione*, cit., 308. Cfr. anche la ricostruzione contenuta in W.L. Prosser, *Privacy*, cit., 384-388 e giurisprudenza *ivi* richiamata.

[6] W.L. Prosser, *Privacy*, cit., 389. che precisa come ciò che è comunemente ricondotto al diritto alla *privacy* « *is non one tort, but a complex of four. The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley, ''to let be alone''* » (le parole citate dall'A. sono di T. Cooley, *Torts*, Chicago, 1888, 91, che per primo avrebbe ipotizzato l'esistenza di un « diritto ad essere lasciato solo »). *Contra* cfr. E.J. Bloustein, *Privacy as an aspect of human dignity: an answer to Dean Prosser*, in *New York University Law Review*, vol. 39, 1964, 962 ss.

del pubblico e, infine, dall'appropriazione a scopo di lucro del nome o della immagine altrui[7].

È con il caso *Griswold*[8] che, in seguito, si è però accolta definitivamente l'idea che il *right to privacy* — anche se non esplicitamente previsto — sia un diritto di rango costituzionale « garantito, indirettamente, non già da una sola disposizione ma da più norme costituzionali, che riconoscono i diritti fondamentali del cittadino »[9], fra cui quelle contenute negli emendamenti I, IV, V e IX che tutelano rispettivamente la libertà negativa di manifestazione del pensiero, il domicilio, la garanzia contro l'autoincriminazione, i diritti che il popolo americano si è « trattenuto »[10].

Senza *privacy* non potrebbe « esservi libera scelta e libera decisione », per cui la sua funzione sarebbe quella di « costituire un'immunità da ogni interferenza esterna, che possa modificare o influenzare i termini delle scelte, che ogni uomo deve compiere liberamente »[11]. Ecco perché nell'ordinamento americano essa è stata progressivamente associata e collegata con « l'intera area dei diritti di libertà »[12], di cui costituirebbe il « fondamento »[13].

Metaforicamente funzionerebbe come una sorta di barriera protettiva nei confronti dei poteri pubblici — ma anche privati — tutelando l'intangibilità della sfera personale in senso bi-direzionale: dall'interno garantisce che l'individuo, in quanto unico titolare di fatti, vicende, dati, pensieri, emozioni attinenti alla propria vita relazionale, decida se e come farli conoscere all'esterno o divulgarli al pubblico; dall'esterno impedisce a terzi di intervenire e interferire con le vicende private del singolo influenzandone le scelte. È in questo modo che nella giurisprudenza statunitense si è spianata la strada ad interpretazioni estensive del diritto *de quo*, ricavando dal diritto alla *privacy* la copertura costituzionale per altri e diversi diritti come quello all'uso dei contraccettivi, al possesso di materiale pornografico fino allo stesso *diritto di aborto*[14], in quanto attinenti alla sfera

---

[7] W.L. Prosser, *Privacy*, *cit. loc. cit.*

[8] Si tratta di *Griswold v. Connecticut*, 381 U.S. 476, 1965 relativo alla legittimità di una legge costituzionale che vietava l'uso dei contraccettivi nei rapporti coniugali.

[9] A. Baldassarre, *op. cit.*, 323. Per una ricostruzione della giurisprudenza americana in materia cfr. anche A. Cerri, *Riservatezza (diritto alla)*, *II) Diritto comparato e straniero*, in *Enc. giur.*, Roma, 2003, 3-6.

[10] Il vocabolo costituisce la parafrasi del predicato utilizzato nel IX emendamento anche se, in verità, la traduzione italiana non rende appieno il senso della disposizione americana che si riporta nella versione originale: « *The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people* »

[11] A. Baldassarre, *op. cit.*, 156 che riassume le parole del giudice Douglas nella nota *dissentig opinion* della controversia *Public Utilities Commision of the District of Columbia v. Pollak* (cfr. in part. pp. 153-158 e bibliografia *ivi* citata).

[12] A. Baldassarre, *op. cit.*, 458 (ma *passim*) che in seguito precisa: « La *privacy*, in altri termini, più che un diritto di libertà o più che il diritto alla libertà, è una nuova ''dimensione'' dei diritti di libertà stessi, resa necessaria dai mutamenti istituzionali comportati dalle moderno democrazie di massa e dall'evoluzione scientifica, per la quale la ''coscienza'' non è più in gran parte un mistero » (in part. p. 473).

[13] Id., *op. cit.*, 471.

[14] Sulla ricostruzione dell'evoluzione della giurisprudenza americana in materia e per una critica alla riconduzione del diritto di aborto alla *privacy* postulando un esercizio troppo discrezionale del *balancing test* A. Baldassarre, *op. cit.*, 332-357, ma cfr. anche pp. 474-475.

personale del soggetto ed alla sua autonoma autodeterminazione in cui lo Stato non dovrebbe intervenire né incidere sulla libertà di scelta[15].

Preme, inoltre, evidenziare come, paradossalmente, nonostante l'accoglimento di un concetto di *privacy* così ampio, un altro diritto come quello alla protezione dei dati personali, che è una sua diretta derivazione, non riceve oltreoceano una protezione statale di carattere complessivo. Le scelte governative mirano a regolare solo specifici settori perché una protezione troppo intensa potrebbe limitare la libertà di iniziativa economica[16]. L'idea americana è che siano gli stessi soggetti che raccolgono e gestiscono i dati personali a dover autoregolamentarsi; saranno poi i consumatori, sulla base del valore che danno alla proprie informazioni, a scegliere il gestore o l'impresa che assicurino un maggior grado di tutela della propria *privacy*: la formazione di banche dati private è considerata, dunque, più un problema di 'mercato' che una questione politica[17].

2. *Privacy* e riservatezza: un rapporto di genere a specie. Il fondamento costituzionale del diritto alla riservatezza nell'ordinamento italiano.

Nell'ordinamento italiano il dibattito sull'esistenza di un omologo diritto alla *privacy* si è aperto intorno agli anni Cinquanta, ma non si è riuscito a coniare, né in dottrina né in giurisprudenza, un termine capace di riassumere in sé l'amplissimo contenuto della categoria statunitense[18]. Il diritto alla riservatezza[19], il diritto ad essere lasciato solo[20], il diritto alla tranquillità individuale[21] o il rispetto della vita privata sono solo degli aspetti della più generale *privacy* attraverso la quale « l'individuo è genericamente protetto contro l'ingerenza altrui nella propria vita privata »[22] e nella « quale rientrano, secondo la dottrina americana prevalente, l'interesse al segreto, alla tranquillità, all'identità personale, all'immagine, al non uso del nome e del ritratto per scopi commerciali »[23].

---

15 In tal senso la *privacy* viene configurata come « sfera di ''immunità'' rispetto al controllo sociale » (A. Cerri, *Riservatezza (diritto alla)*, *II) Diritto comparato e straniero*, cit., 6.

16 S. Nespor-A.L. De Cesaris, *Internet e la legge*, Milano, 2001, 89 ss.

17 M. Adenas-S. Zleptnig, *Surveillance and Data protection: Regulatory approaches in the EU and Member States*, in *European Business Law Review*, 766, che, a conferma della tesi esposta, ricorda la diatriba instauratasi fra Unione europea e Stati Uniti con riguardo alle divergenze originate dal trasferimento dei dati dei passeggeri dei voli transoceanici.

18 T.A. Auletta, *Riservatezza e tutela della personalità*, Milano, 1978, 26-27.

19 Cfr., *ex plurimis*, T.A. Auletta, *Riservatezza e tutela della personalità*, cit.; A. Cerri, *Riservatezza (diritto alla)*, *III) Diritto costituzionale*, in *Enc. giur.*, Roma, 1995, 1 ss.; G. Giacobbe, *Riservatezza (diritto alla)*, in *Enc. dir.*, Milano, 1989, 1243 ss.

20 P. Rescigno, *Il diritto di essere lasciati soli*, in A. Guarino-L. Labruna (a cura di), *Synteleia per V. Arangio Ruiz*, Napoli, 1964, 494 ss.

21 M. Atelli, *Il diritto alla tranquillità individuale*, Napoli, 2001.

22 T.A. Auletta, *Riservatezza e tutela della personalità*, cit., 27.

23 T.A. Auletta, *Riservatezza e tutela della personalità*, cit., 27-28. Cfr. anche E. Roppo, *I diritti della personalità*, in G. Alpa-M. Bessone (a cura di), *Banche dati, telematica e diritti della persona*, Padova, 1981, 62, che sostiene come il « *Right to privacy* [sia], nell'esperienza del diritto

La giurisprudenza italiana, dal proprio canto, ha in un primo momento escluso l'esistenza di un generale diritto alla vita privata sulla base della mancata menzione di esso in Costituzione, ed ha ammesso successivamente l'esistenza del diritto alla riservatezza anche sulla scorta della posizione espressa dalla Corte Costituzionale che lo ha incluso — insieme al diritto al decoro, all'onore, alla propria rispettabilità, all'intimità e alla reputazione — fra i diritti inviolabili di cui all'art. 2 Cost.[24]

Il diritto alla riservatezza — inteso come « l'interesse alla non conoscenza [...] delle vicende personali »[25] — viene così comunemente utilizzato per tradurre il *right to privacy* anche se — come già messo in evidenza — ne costituisce solo una parte. Esso è annoverato fra i cc.dd. ''nuovi diritti'': ovvero fra quei diritti non espressamente previsti in Costituzione ma entranti a far parte del nostro ordinamento attraverso la clausola contenuta nell'art. 2 Cost.[26] che riconosce i diritti inviolabili dell'uomo[27] e consente — al fine di garantire l'adeguamento al cambiamento della sensibilità e delle esigenze della collettività — una interpretazione evolutiva dei diritti contenuti nello stesso catalogo costituzionale[28].

Il suo fondamento costituzionale si rinviene in quegli articoli della Costituzione che tutelano « specifiche sfere di libertà individuale dall'altrui ingerenza »[29] come la libertà personale, l'inviolabilità domiciliare o la segretezza della corrispondenza; nonché in quelli dove si « fa espresso riferi-

americano, concetto di amplissimo spettro che rinvia a significati anche molto diversi tra loro coprendo tutta una serie di interessi, prerogative, aspettative e pretese del singolo, attinenti alla sfera della sua persona o personalità, e muniti di tutela legale. Sotto questo profilo, una traduzione di esso in termini di ''diritto generale della personalità'' sarebbe certo più appropriata che non una traduzione in parole di semplice ''diritto alla riservatezza'': parole queste che suonerebbero davvero riduttive a fronte dell'intensità e della ricchezza semantiche sprigionate dalla formula della ''*privacy*''». Concorde sul fatto che il complesso significato del termine *privacy* non sia completamente reso da alcuna parola italiana e che le relative traduzioni si limitano a coglierne solo alcuni aspetti G. Alpa-M. Bessone, *Introduzione*, in Id. (a cura di), *Banche dati, telematica e diritti della persona*, cit., 4-5.

[24] Corte Cost. 12/4/1973 n. 38 (punto 2 c.d.), in *Giur. cost.*, 1973, 362. Per una più approfondita analisi dell'evoluzione giurisprudenziale in materia cfr. T.A. Auletta, *op. cit.*, 62-66; A. Cerri, *Riservatezza (diritto alla), III) Diritto costituzionale*, cit., 2 ss.; P. Menga, *Banche dati, diritto alla riservatezza e telematica*, in *Giur. it.*, 1999, 1351 ss.; G.M. Salerno, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. Nania-P. Ridola (a cura di), *I diritti costituzionali*, vol. II, Torino 2001, 444 ss.; F. Bilotta, *L'emersione del diritto alla privacy*, in A. Clemente (a cura di), *Privacy*, Padova, 1999, 41 ss.; G. Alpa-M. Bessone (a cura di), *Introduzione*, in Id., *Banche dati, telematica e diritti della persona*, cit., 13 ss.

[25] T.A. Auletta, *op. cit.*, 28.

[26] P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984. 61.

[27] Per un approfondimento ed una lineare panoramica degli orientamenti dottrinali sul problema del fondamento positivo o extrapositivo del riconoscimento dei diritti inviolabili contenuto nell'art. 2 Cost. A. Baldassare, *Diritti della persona e valori costituzionali*, Torino, 1997, 21 ss.

[28] Sul tema dell'apertura del nostro ordinamento a diritti non espressamente enumerati nella Carta costituzionale, *ex plurimis*, F. Modugno, *I nuovi diritti nella giurisprudenza costituzionale*, Torino, 1995; A. Pace, *Problematica delle libertà costituzionali*, Padova, 2002; P. Barile, *Diritti dell'uomo e libertà fondamentali*, cit.; A. Barbera, *Commento all'art. 2*, in G. Branca (a cura di), *Commentario alla Costituzione*, Bologna, 1975, 80 ss.; N. Bobbio, *L'età dei diritti*, Torino, 1997; V. Angiolini (a cura di), *Libertà e giurisprudenza costituzionale*, Torino, 1992.; A. Baldassare, *Diritti della persona e valori costituzionali*, cit.

[29] G.M. Salerno, *La protezione della riservatezza*, cit., 423.

mento a situazioni, rapporti o comunque ambiti di attività umane giuridicamente protetti da interferenze esterne »[30] come « il diritto all'esercizio in privato del culto religioso (art. 19), il diritto al nome (art. 22), l'inviolabilità del diritto di difesa (art. 24), i diritti della famiglia come società naturale (art. 29 ss.), ed il rispetto della persona umana nell'assoggettamento ai trattamenti sanitari obbligatori (art. 32) »[31].

Si tratterebbe, da questo punto di vista, di un diritto *implicito/trasversale*[32] ricavabile attraverso un'interpretazione estensiva-sistematica delle disposizioni citate[33].

L'interesse costituzionale alla tutela della vita intima e privata della persona, d'altronde, sembra essere ''logicamente sottinteso'' nella nostra Carta costituzionale, apparendo *strumentale* alla realizzazione di ulteriori valori cui esso è connesso. In altre parole, si desidera porre l'accento sul fatto che garantire la riservatezza nell'ordinamento italiano — così come garantire la *privacy* nell'ordinamento americano — vuole dire *tutelare la persona*, consentire il suo libero sviluppo e l'esercizio di diritti costituzionalmente sanciti di cui rappresenta la 'precondizione'. Significa, in altre parole, consentire il pieno esercizio del proprio diritto all'autodeterminazione individuale[34] e della propria libertà di scelta[35], compromesse nel momento in cui idee o vicende private che l'individuo ha interesse a non divulgare in determinati ambienti « nei quali sarebbero causa di riprovazione o addirittura di discriminazione e, nei casi più gravi, di esclusione da essi »[36] escano dalla propria disponibilità. In casi siffatti si realizza — oltretutto e conseguentemente — un possibile ostacolo all'esercizio di altre libertà costituzionali come, fra le altre, la riunione, l'associazione, la « professione religiosa » che « potrebbero risultare compromesse dalla pubblicizzazione di certe notizie »[37].

L'indebita intrusione nella vita altrui animata dalla curiosità di terzi estranei, la conservazione e divulgazione di informazioni personali senza il consenso dell'avente diritto ledono il *diritto* del singolo di decidere liberamente quanto della propria personalità comunicare al pubblico. I motivi che spingono a non rivelare le proprie informazioni possono essere della natura più varia: dal semplice riserbo personale a ragioni di ordine contingente, come la consapevolezza che la conoscenza di determinate informazioni sul proprio conto può essere fonte di disparità di trattamento o anche

---

[30] G.M. Salerno, *op. cit.*, 424. Sul punto cfr. anche le considerazioni di F. Modugno, *op. cit.*, 20 ss.

[31] G.M. Salerno, *op. cit. loc. cit.*

[32] Sulla distinzione dei ''nuovi diritti'' in diritti impliciti, trasversali e strumentali F. Modugno, *op. cit.*, 2.

[33] *Contra* A. Pace, *Interpretazione costituzionale e interpretazione per valori*, in G. Azzariti (a cura di), *Interpretazione costituzionale*, Torino, 2007, 107 ss. che nega l'esistenza di un *unitario* diritto costituzionale alla riservatezza sostenendo che vi siano quattro diverse problematiche — attinenti rispettivamente, ai limiti all'accesso di fonti notiziari private, ai limiti alla divulgabilità di notizie private, alla tutela dei segni distintivi e alla disciplina delle banche dati nonché, infine, al trattamento automatizzato dei dati — aventi diversi « referenti costituzionali ».

[34] T.A. Auletta, *op. cit.*, 34.

[35] F. Modugno, *op. cit.*, 19-20, che ricostruisce la libertà di scelta e la libertà di coscienza come aspetti della libertà morale o spirituale le quali hanno il proprio fondamento nell'art. 13 Cost. L'A. citato sostiene, infatti, che l'inviolabilità personale debba essere intesa, oltre che come tutela dell'integrità fisica, anche come tutela dell'integrità psichica o spirituale in quanto « sua precondizione necessaria » (p. 19).

[36] T.A. Auletta, *op. cit.*, 34.

[37] T.A. Auletta, *op. cit.*, 35.

di ricatto. La Costituzione, anche se indirettamente, riconosce tali esigenze e le tutela sotto forma di diritti fondamentali garantiti dall'art. 13 e dall'art. 21 Cost., come diritto all'integrità psichica (o morale)[38] e come libertà negativa di manifestazione del proprio pensiero[39].

È in questa accezione che riemerge in tutto il suo contenuto deontico il cd. diritto all'identità individuale[40], inteso come prerogativa di disporre autonomamente del patrimonio ideale emotivo costituito dalle proprie esperienze e dalle informazioni, dai fatti, dai dati che ad esse si riferiscono. *A contrario*, si realizzerebbe una irragionevole distinzione fra cittadini nell'esercizio della libertà scelta e di diritti come quello all'autodeterminazione o all'identità individuale; ma anche nell'esercizio di altre libertà fondamentali che il cittadino non potrebbe esercitare pienamente qualora, per fare un esempio banale, avesse il timore che la conoscenza delle proprie informazioni personali e dei propri dati sensibili[41] possa compromettere la partecipazione ad una comunità, ad un'associazione, ad una riunione o possa impedire il libero esercizio della manifestazione del pensiero. In tutti questi casi ad essere leso è proprio il principio di eguaglianza nella veste della pari dignità sociale di cui all'art. 3 Cost. il quale postula che « i pubblici poteri siano obbligati ad operare affinché *tutti possano godere in modo equiordinato dei diritti fondamentali* »[42].

La tutela della riservatezza e della vita intima dell'individuo è, dunque, parte della più generale garanzia della ''personalità umana'' intesa « come valore spirituale ed etico » che informa « secondo le leggi universali della dignità umana » il « sistema dei diritti e dei doveri costituzionali »[43]. La dignità umana rappresenta, in tal senso, il concetto di sintesi del contenuto sostanziale della personalità umana che « orienta » e « indirizza » la vita dell'ordinamento stesso[44]. Se una tutela non adeguata delle informazioni individuali e relazionali può, come visto, pregiudicare l'esercizio di altri diritti fondamentali costituzionalmente tutelati è proprio la dignità

---

[38] F. MODUGNO, *op. cit.*, 19. Ma precedentemente anche C. MORTATI, *Istituzioni di diritto pubblico*, Padova, 1976, vol. II, 1040-1401, che, esaltando il ruolo della libertà personale « che condiziona tutte le altre [libertà] rendendone possibile l'esplicazione », evidenzia come essa si sostanzi non solo nell'integrità fisica della persona ma anche in quella psichica, mirando a sottrarre l'uomo da 'coercizioni' che possano « defor[mare] artificialmente i naturali processi psichici dell'individuo ».

[39] P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., 231-232, che la definisce come « libertà di tacere ».

[40] Sui diritti di identità individuale F. MODUGNO, *op. cit.*, 13 ss. Al contrario, nega che il diritto all'identità personale abbia fondamento costituzionale S. FOIS, *Questioni sul fondamento costituzionale del diritto all'« identità personale »*, in G. ALPA-M. BESSONE-L. BONESCHI-G. CAIAZZA (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, 155 ss.

[41] Si tratta dei « dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale » (d.lgs. 196/03, art. 4, co. 1, lett. *d*).

[42] G.M. SALERNO, *op. cit.*, 437 (corsivi nostri).

[43] A. BALDASSARRE, *Libertà*, in *Enc. giur.*, Roma, 1990, 20, che, con il concetto descritto — ribadendo l'abbandono a partire dagli anni Trenta della « concezione ''economicistica'' della personalità umana » — evidenzia il passaggio dal binomio ''libertà-proprietà'', per cui la libertà è intesa come « libera proprietà sul proprio corpo », al binomio ''libertà-dignità umana'' « implicante la tutela dell'habeas mentem a fianco dell'habeas corpus ».

[44] A. BALDASSARRE, *Libertà*, cit., 21.

umana ad essere lesa poiché questa rappresenta, secondo la dottrina richiamata, la « misura [...] dell''*ethos* ideale della persona'' » il cui contenuto « positivo-normativo » è rappresentato proprio dal riconoscimento delle libertà fondamentali[45].

3. L'affermazione delle nuove tecnologie informatiche e delle banche dati telematiche: il problema della determinazione del contenuto del diritto alla riservatezza in rapporto con altri interessi costituzionalmente rilevanti.

Le considerazioni svolte risultano valide e drammaticamente attuali sol che si pensi allo sviluppo delle nuove tecniche di acquisizione nonché di conservazione dei dati e delle informazioni personali.

L'affermazione delle moderne tecnologie informatiche offre indubbiamente rilevanti opportunità per lo sviluppo della personalità del singolo, consentendo l'acquisizione e lo scambio di informazioni dal contenuto e dalla natura più vari. Tuttavia, man mano che si facilitano forme generalizzate di raccolta dei dati, aumentano anche i rischi per la riservatezza delle persone[46]. Le memorie sempre più capienti dei moderni elaboratori, la possibilità di conservare i dati per periodi di tempo pressoché illimitati, la capacità dei programmi informatici di identificare i singoli attraverso il trattamento dei dati personali, l'opportunità di raffrontare le diverse banche dati[47] contenenti informazioni sulle abitudini sociali, creano un continuo e concreto rischio per l'identità personale[48] del cittadino, la quale finisce con l'essere completamente « affidata al modo in cui le informazioni vengono trattate, collegate e fatte circolare »[49].

---

[45] *Ibidem*.

[46] Per un'analisi del fenomeno anche dal punto di vista sociologico si rinvia a D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, trad. it. A. Zanini, Milano, 2002, che ritiene peculiare caratteristica delle « cosiddette società dell'informazione » il fatto di essere necessariamente « società sorvegliate » (in particolare p. 6). Sul problema della tutela della riservatezza dopo l'avvento della nuove tecnologie V. Franceschelli (a cura di), *La tutela della privacy informatica*, Milano, 1998; G. Buttarelli, *Banche dati e tutela della riservatezza*, Milano, 1997.

[47] Sulla nozione di banca dati e sui principi costituzionali coinvolti G. Rao, *Informatica, banche dati e principi costituzionali*, in AA.VV., *Nuove dimensioni nei diritti di libertà (Scritti in onore di Paolo Barile)*, Padova, 1990, 473 ss. Cfr. anche R.G. Rodio, *Profili ricostruttivi del concetto di archivio elettronico e di banca dati*, in A. Loiodice-G. Santaniello (a cura di), *La Tutela della riservatezza*, *Trattato di diritto amministrativo*, diretto dal G. Santaniello, vol. XXVI, Padova, 2000, 555; R. Pagano, *Aspetti economici e giuridici delle banche dati*, in G. Alpa-M. Bessone (a cura di), *Banche dati, telematica e diritti della persona*, cit., 105 ss.

[48] L'identità personale, infatti, riguarderebbe soprattutto « il modo con cui un soggetto viene presentato ''agli occhi del pubblico'' attraverso l'insieme delle informazioni che lo riguardano ». Così S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, 109. Sul concetto di identità personale si rinvia, fra le opere più recenti, a G. Pino, *Il diritto all'identità personale*, Bologna, 2003. Sul tema cfr. anche A. Scalisi, *L'identità personale*, in Id., *Il valore della persona nel sistema e nuovi diritto della personalità*, Milano, 1990; 143 ss. e bibliografia *ivi* richiamata in nota 1; S. Miarelli, *Il diritto all'identità personale*, in A. Clemente (a cura di), *Privacy*, cit., 75 ss.

[49] S. Rodotà, *Una scommessa impegnativa sul terreno dei diritti*, discorso del Presidente dell'Autorità Garante per

Se un soggetto è costantemente tenuto sotto il controllo di terzi estranei (peggio se a sua insaputa), per cui le informazioni che lo riguardano — e che gli appartengono — non sono più nella sua disponibilità, cessa di essere padrone della propria 'individualità'[50]. Ogni soggetto di diritto è titolare delle informazioni — di qualsiasi natura — che lo riguardano perché esse contribuiscono a trasformare la persona in ''un individuo'' ovvero in qualcosa di *unico* che lo distingue dagli altri soggetti. Non avere più la disponibilità di quelle informazioni significa perdere qualcosa della propria individualità ed essere lesi nella propria libertà/dignità[51]. Ad essere violata è in questi casi la *libertà di scelta* della persona di decidere se e cosa della propria personalità rendere disponibile a terzi; e tale libertà — strettamente connessa con la libertà di coscienza ed intesa come un aspetto della libertà morale o spirituale — è « forse l'aspetto della personalità in cui si manifesta più intensamente il valore della *dignità umana* »[52]. Se nel linguaggio comune il termine dignità indica « lo stato complessivo in cui si trova chi gode del rispetto, dell'onore e della stima (altrui e/o propria) »[53], la dignità umana sarebbe, secondo parte della dottrina, « una qualità *intrinseca* della condizione umana »[54] implicitamente presupposta in tutta una serie di disposizioni costituzionali — come, fra le altre, quelle che vietano violenze fisiche o morali nei confronti dei soggetti sottoposti a misure restrittive, quelle relative ad divieto di pene contrarie al senso di umanità, quelle inerenti il diritto degli inabili e dei minorati al mantenimento all'assistenza *etc.* —[55] costituendo il « fine » ed allo stesso tempo il « con-fine » delle libertà costituzionalmente garantite[56]. Un richiamo a questi valori è d'altronde contenuto nello stesso codice per la protezione dei dati personali — di cui si dirà[57] — stabilendo che tutti

la protezione del dati personali tenuto il 18 maggio 2001 alla presentazione della Relazione per il 2001, in *http://www.interlex.it/675/rodota6.htm*.

[50] In tal senso, E.J. Bloustein, *Privacy as an aspect of human dignity: an answer to Dean Prosser*, cit., 1003

[51] E.J. Bloustein, *op. loc. cit.*, che espressamente afferma « *The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinion, being public, tend never to be different; is aspiration, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual* ». Vd. anche le considerazioni di F. Modugno, *op. cit.*, 22 ss.

[52] F. Modugno, *I nuovi diritti nella giurisprudenza costituzionale*, cit. 23. Si ricorda, a tal proposito, che nell'ordinamento tedesco, in mancanza di espliciti riferimenti nella Legge fondamentale, il diritto alla riservatezza viene desunto proprio dalle norme che garantiscono la dignità dell'uomo ed il pieno sviluppo della persona (A. Cerri, *Riservatezza (diritto alla), II) Diritto comparato e straniero*, cit., 7).

[53] A. Ruggeri-A. Spadaro, *Dignità dell'uomo e giurisprudenza costituzionale (prime notazioni)*, in *Pol dir.*, 1991, 344.

[54] *Ibidem* (corsivi nel testo).

[55] La tesi ricordata e gli esempi descritti sono tutti di A. Ruggeri-A. Spadaro, *op. cit.*, 345-346.

[56] Id., *op. cit.*, 347. Da questo punto di vista, la dottrina citata ricostruisce la dignità umana alla stregua di un « valore supercostituzionale » che costituirebbe la « norma di chiusura » del nostro ordinamento in quanto fine superiore « *sussuntivo e fondante* la natura teleologicamente personalista del nostro ordinamento » (pp. 347-348, cfr. anche pp. 355, 367, 370).

[57] Cfr. *infra* parr. 6 ss.

i trattamenti di dati personali debbano essere effettuati nel rispetto « della dignità dell'interessato »[58].

Per quanto interessa questa sede, le schedature di massa ''compongono in sistema'' abitudini e comportamenti. Consentono di tracciare dei fili conduttori fra caratteristiche, condotte, atteggiamenti dei soggetti; mirano a creare modelli di identità comuni ai più, con la potenziale — ma probabile e paradossale — conseguenza di creare la diffidenza e di far temere chi si discosta dal modello tenuto dalla maggioranza[59]. Tendono ad imporre l'identità collettiva cui i singoli dovrebbero omologarsi per non essere considerati 'sospetti'[60], negando l'individualità e l'identità *individuale*.

Il problema non è sicuramente nuovo nel dibattito giuridico italiano. Già negli anni Settanta, autorevole dottrina metteva in guardia dai rischi derivanti dalla costituzione delle banche dati informatiche che, consentendo la conservazione ed il confronto di informazioni personali, avrebbero creato una sorta di « giudizio universale permanente ed incombente, per cui ogni individuo schedato elettronicamente può essere sottoposto ad una sorveglianza continua e inavvertita degli atti rilevanti della sua vita privata »[61].

La diffusione dei processori e la formazione di archivi elettronici ha posto immediatamente il problema della difesa nei confronti del nuovo « potere informatico »[62] dei soggetti pubblici e privati titolari del trattamento automatizzato delle informazioni riguardanti il singolo.

I diritti e le libertà fondamentali, allora, devono oggi essere ricostruiti alla luce delle nuove tecniche informatiche e telematiche, e l'inviolabilità della persona non può essere più limitata al solo « corpo fisico », ma deve estendersi anche a quello « elettronico »[63]. Come è stato evidenziato, infatti, l'esistenza di archivi informatici di natura diversa e la possibilità di trattare in vario modo i dati individuali contribuirebbero a trasformare la persona in « un'entità disincarnata » costituita dalle informazioni che la riguardano[64]. Tutelare la *privacy* significa allora anche garantire di non essere « costruiti »[65] dagli altri attraverso i dati

---

58 D.lgs. 196/2003, art. 2.

59 Cfr. le considerazioni di S. RODOTÀ, *Intervista su* privacy *e libertà*, Roma-Bari, 2005, 29 ss.

60 Nel senso che il controllo generalizzato delle persone attraverso la conservazione dei dati personali attuato anche attraverso le nuove tecnologie di sorveglianza (telecomunicazioni, biometria, videosorveglianza *etc.*) contribuiscano a creare la « cultura del sospetto », D. LYON, *Massima sicurezza. Sorveglianza e ''guerra al terrorismo''*, tr. it. E. Greblo, Milano, 2005, 40, 54 ss. ma *passim*.

61 V. FROSINI, *Introduzione*, in S. SIMITIS, *Crisi dell'informazione giuridica ed elaborazione elettronica dei dati*, Milano, 1977, 1. Sul punto cfr. anche M.G. LOSANO, *Il diritto pubblico dell'informatica. Corso di informatica giuridica*, II/2, Torino, 1992, che, riprendendo un'espressione nata nei paesi scandinavi, utilizza la metafora della « sindrome del pesce rosso » per i singoli continuamente spiati in una « società trasparente » in cui ognuno è costantemente ed inevitabilmente osservato come in una « boccia di cristallo » (p. 13).

62 V. FROSINI, *Diritto alla riservatezza e calcolatori elettronici*, in G. ALPA-M. BESSONE (a cura di), *Banche dati, telematica e diritti della persona*, cit., 29.

63 In tal senso, S. RODOTÀ Discorso alle Camere del Presidente dell'Autorità garante per la presentazione della Relazione 2003, in *www.garanteprivacy.it*, in part. p. 17.

64 S. RODOTÀ, *Una scommessa impegnativa sul terreno dei diritti*, cit.

65 S. RODOTÀ, *ult. op. cit.*

che ci riguardano: lo sviluppo della persona umana presuppone necessariamente oltre il riconoscimento dell'*habeas corpus* anche quello dell'*habeas data*[66].

Alla luce di queste considerazioni, deve essere osservato che, anche se il diritto alla riservatezza ed il diritto alla protezione dei propri dati personali — che *promana* logicamente dal primo — sono diritti fondamentali, la loro ampiezza ed i relativi limiti si determinano attraverso l'esame della relativa collocazione all'interno del sistema dei valori costituzionali in cui si inseriscono. In altre parole, si tratta di capire quale sia l'effettivo raggio d'azione del generale diritto alla vita privata in ragione del bilanciamento con gli altri interessi e beni costituzionali con cui viene a relazionarsi e con cui deve comporsi[67]. La questione non attiene solamente all'annoso, quanto intricato, rapporto fra il diritto alla riservatezza e quello alla libertà di manifestazione del pensiero, ma — soprattutto con riferimento alla formazione delle banche dati — fra il primo ed altri interessi fondamentali come l'esigenza di semplificazione dell'attività amministrativa, la libertà di informazione e di ricerca delle informazioni, la sicurezza, l'ordine pubblico. A questo deve essere aggiungersi come il bilanciamento descritto cambia a seconda della fattispecie, del tipo di dato che si vuole conservare, del particolare momento storico e anche del mezzo tecnico utilizzato per l'acquisizione. Ciò perché plurime sono le soluzioni rese possibili dal complesso sistema dei valori costituzionali coinvolti; si tratterà, allora, di trovare caso per caso il 'ragionevole' punto di equilibrio fra i diversi beni fondamentali.

Ad esempio, è indubbio che debba esservi una tutela più intensa per i dati sensibili[68] perché si tratta di informazioni che con maggiore facilità possono dar luogo a ingiuste discriminazione fra i singoli; che debbano essere comunicati i propri dati anagrafici ai pubblici poteri per esigenze di semplificazione ed efficienza della funzione amministrativa; che in determinati momenti storici la tutela della riservatezza della persona possa essere, temporaneamente, affievolita per ragioni legate alla sicurezza collettiva. In tutti questi casi, però, bisognerà sempre valutare se il bilancia-

[66] S. Rodotà, *ult. op. cit.*; V. Frosini, *op. cit. loc. cit.*; G.B. Ferri, *Privacy e libertà informatica*, cit., 51.

[67] Si utilizza, in tal senso, la terminologia contenuta in P. Häberle, *Le libertà fondamentali nello Stato costituzionale*, tr. it. A. Fusillo-R.W. Rossi, Roma, 1993, *passim*, dove si sostiene come fra i diversi beni costituzionali sussistono rapporti di « reciproco condizionamento »; tuttavia, più che conflitto, fra loro vi sarebbe « complementarità » per cui i « limiti e il contenuto dei diritti fondamentali devono essere determinati tramite una ''visione d'insieme'' che tenga conto del significato che hanno questi diritti quali elementi costitutivi di un sistema unitario. Nessuna norma costituzionale può essere interpretata come a sé stante » (in part. pp. 39-40). Come è stato, anche dalla dottrina italiana, ben evidenziato, i valori costituzionali costituiscono « un universo politeistico, che, soltanto in seguito al bilanciamento dei singoli valori fra loro, alla loro strutturazione gerarchica e al conseguente superamento delle relative antinomie, può presentarsi, sempreché sia correlato a una fattispecie determinata (attività tipizzata), come un sistema dal quale si può trarre una massima di decisione » (A. Baldassarre, *Libertà*, cit., 23). Molto numerosi sono i contributi della dottrina italiana sul tema con tesi e punti di osservazione diversi: cfr., per tutti, R. Bin, *Diritti e argomenti. Il bilanciamento degli interessi nella giurisprudenza costituzionale*, Milano, 1992; A. Baldassare, *Diritti della personale e valori costituzionali*, Torino, 1997; R. Rimoli, *Pluralismo e valori costituzionali. I paradossi dell'integrazione democratica*, Torino, 1999.

[68] Cfr. definizione contenuta *supra* in nota 41.

mento operato dal legislatore rispetto alle diverse opzioni possibili, sia « plausibi[le] e non arbitrar[io] rispetto al risultato prefissato dalla stessa norma » attraverso il « giudizio di ragionevolezza » sulla legge[69].

Rimane ancora da sottolineare come il diritto alla riservatezza del singolo, anche nelle ipotesi descritte in cui è ammessa la conservazione dei dati personali, non può, comunque, essere sacrificato del tutto ma è compensato dal riconoscimento del diritto « di conoscere, controllare, indirizzare, interrompere il flusso delle informazioni che lo riguardano »[70]. Ecco perché la tutela della *privacy* è stata progressivamente collegata con « l'insieme delle libertà implicate nel trattamento dei dati personali »[71], ampliandosi dei nuovi significati « di affermazione della propria libertà e dignità della persona, di limitazione imposta dall'individuo sul potere informatico, di controllo attivo del mezzo e del fine di quel potere »[72]. In tale contesto, si invoca il riconoscimento di una nuova « libertà informatica »[73] consistente nel potere di controllare le proprie informazioni personali ricadute nella disponibilità di terzi.

4. Internet come nuovo mezzo di raccolta e diffusione delle informazioni degli utenti. I beni giuridici informatici e tutela del cd. ''domicilio informatico''.

Con l'affermazione delle nuove forme di comunicazione globale, inoltre, il tema, già tanto dibattuto, della tutela della riservatezza nel nostro ordinamento si ripropone con diversi contenuti a cagione delle peculiari caratteristiche tecniche del mezzo utilizzato che giustificano una separata ed apposita analisi.

Il riferimento è, nello specifico, alla diffusione del fenomeno Internet, nel contesto del quale, il problema della *privacy* si accentua dato che le occasioni di disturbo e di lesione della sfera intima e personale del singolo si moltiplicano esponenzialmente con modalità del tutto innovative che ne-

---

[69] A. Baldassarre, *Libertà*, cit., 23.

[70] S. Rodotà, *ult. op. cit. loc. cit.*; sul punto anche Id., *Tecnologie e diritti*, cit., 33, 47 (ed indicazioni bibliografiche *ivi* in nota 7), 79, 80, 101, 122. Sul punto cfr. disposizioni del Decreto legislativo 30 giugno 2003, n. 196 (Codice della Privacy) su cui *infra* parr. 6 ss.

[71] S. Rodotà, *Prefazione*, in D. Lyon, *La società sorvegliata*, cit., pp. VIII e X; sul tema vd anche R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003.

[72] V. Frosini, *Diritto alla riservatezza e calcolatori elettronici*, cit., 33. Sul cambiamento del concetto di *privacy* da garanzia della sfera privata del singolo a *controllo* delle proprie informazioni personali ricadute nella disponibilità dei terzi S. Rodotà, *Progresso tecnico e problemi istituzionali nella gestione delle informazioni*, in Matteucci (a cura di), « *Privacy* » *e banche dati*, Bologna, 1981, 30; Id., *Tecnologie e diritti*, cit., 33, 47, 103; V. Frosini, *Diritto alla riservatezza e calcolatori elettronici*, cit., 33; sul punto anche L. Chieffi, *Centro elaborazione dati istituito presso il Ministero dell'Interno e tutela della riservatezza*, in *Dir. giur.*, 1986, 955.

[73] V. Frosini, *op. cit. loc. cit.*; Id., *L'orizzonte giuridico dell'Internet*, in questa *Rivista*, 2000, 275. Per un esame del riconoscimento della libertà informatica come « nuova dimensione del diritto di libertà personale » legata allo sviluppo delle tecnologie di comunicazione T.E. Frosini, *Tecnologie e libertà costituzionali*, in *Scritti in memoria di Livio Paladin*, Napoli, 2004, 833, che in proposito riflette anche sugli spunti derivanti dall'esperienza comparata (in part. pp. 836 ss).

cessitano un richiamo alla difesa della riservatezza individuale nel suo più ampio significato di interesse alla non pubblicizzazione delle proprie vicende private e di tutela della sfera intima e personale del singolo[74].

Attraverso il *web* si è amplificata la possibilità di intercettazione ed acquisizione da parte di terzi delle informazioni personali degli utenti[75] su cui anche il legislatore italiano è dovuto intervenire introducendo, fra l'altro, il controverso concetto di ''domicilio informatico''. Analogamente, sono aumentate le occasioni per ottenere informazioni personali — raccolte in maniera non sempre trasparente — che agevolano la formazione di innumerevoli e nuove tipologie di banche dati non necessariamente giustificate da interessi meritevoli di tutela ma potenzialmente lesive dell'identità personale del singolo. A ciò deve aggiungersi che tali dati possono essere trasferiti tramite la rete Internet in qualunque parte le mondo — praticamente a costo zero — rendendo molto più difficile controllare « la circolazione, lo scambio e l'aggregazione delle informazioni » raccolte[76].

I dati informatici — anche per loro intrinseco valore economico di cui si dirà — possono ormai essere considerati come nuovi beni giuridici[77], il cui complesso costituirebbe il « patrimonio informatico »[78] della persona.

---

[74] Molto ampio è il dibattito sulla tutela della riservatezza in rete sul punto S.F. Bonetti, *La tutela dei consumatori nei contratti gratuiti ad accesso ad Internet: i contratti dei consumatori e la* privacy *tra fattispecie giuridiche e modelli contrattuali italiani e statunitensi*, in questa *Rivista*, 2002, 1087; D. Calenda, *Il dibattito internazionale sui limiti e le tendenze delle politiche per la tutela della* privacy *in Internet*, in *Riv. it. dir. pubb. com.*, 2001, 531 ss.; V. Caridi, *La tutela dei dati personali in Internet: la questione dei logs e dei cookies alla luce delle dinamiche economiche dei dati personali*, in questa *Rivista*, 2001, 763 ss.; G. Cassano, *Internet e riservatezza*, in Id. (a cura di), *Internet. Nuovi problemi e questioni controverse*, Milano, 2001, 9; G. Ciacci, *La tutela dei dati personali su Internet*, in A. Loiodice-G. Santaniello (a cura di), *La Tutela della riservatezza*, in *Trattato di diritto amministrativo*, diretto da G. Santaniello, vol. XXVI, Padova, 2000, 369; Id., *Internet e diritto alla riservatezza*, in *Riv. trim. dir. proc. pen.*, 1, 1999, 233; L.M. de Grazia, *Privacy e sicurezza nei contratti online*, in *Trattato breve di diritto della rete* diretto da Siriotti Gaudenzi, Rimini, 2001, 185 ss.; V. Grippo, *Internet e dati personali*, in A. Clemente (a cura di), *Privacy*, Padova, 1999, 285; Id., *Analisi dei dati personali presenti su Internet. La legge n. 675/96 e le reti telematiche*, in *Riv. crit. dir. priv.*, 1997, 639 ss.; R. Imperiali-R. Imperiali, *La tutela della* ''privacy'' *in Internet: difficoltà di un contemperamento*, in *Dir. prat. soc.*, n. 6, 2001, 29 ss.; D. Memmo, *La* privacy *informatica: linee di un percorso normativo*, in *Contratto e impresa*, 2000, 1213; A. Oliva, *La tutela penale del diritto alla* privacy *in Internet*, in *Riv. pen.*, 2002, 91 ss.; P. Pallaro, *La tutela della vita privata in relazione ai trattamenti di dati personali in Internet: l'approccio della Comunità europea*, in *Dir. com. sc. int.*, 2000, 7 ss.; A. Scalisi, *La tutela dei dati personali in rapporto ad Internet*, in Id., *Il diritto alla riservatezza*, Milano, 2002, 303 ss.; L. Stilo, *Internet: crocevia di dati personali*, in *Nuovo diritto*, 2002, fasc. 6, 4 ss.; G.R. Stumpo, *Internet e* privacy*: le misure da adottare per l'utente-consumatore*, in *Dir. e prat. soc.*, n. 1, 2002, 38 ss.; E. Tosi, *Prime osservazioni sull'applicabilità della disciplina generale della tutela dei dati personali a Internet e al commercio elettronico*, in questa *Rivista*, 1999, 591 ss.; N. Visalli, *Contratto di accesso ad Internet e tutela della* privacy, in *Giust. civ.*, II, 2002, 125 ss.

[75] Il fenomeno è quello ormai abbastanza conosciuto degli *hackers* e dei *crackers* telematici, ossia di chi — rispettivamente — viola i sistemi informatici per gioco o dietro pagamento. Sul punto A. Baldassarre, *Globalizzazione contro democrazia*, Roma-Bari, 2002, 250 ss.

[76] V. Caridi, *La tutela dei dati personali in Internet*, cit.,763.

[77] L. Cuomo-B. Izzi, *Misure di sicurezza e accesso abusivo ad un sistema informatico*, in *Cass. pen.*, 2002, 248.

[78] L. Cuomo-B. Izzi, *cit. loc. cit.*; sulla

Uno dei principali problemi sollevati dal fenomeno Internet è costituito proprio dalla lesione che tali « beni giuridici informatici »[79] possono ricevere tramite l'acquisizione, la modifica, il danneggiamento da parte di terzi non autorizzati[80].

Il problema è stato già oggetto dell'intervento del legislatore ordinario che, nel 1993, ha approvato la legge n. 547, inserendo nel codice penale una specifica disciplina per i cosiddetti reati informatici[81].

In particolare, si è espressamente sanzionato, oltre il comportamento di chi autonomamente — o attraverso l'installazione di apposite apparecchiature — intercetta, impedisce o interrompe illecitamente comunicazioni informatiche o telematiche, anche quello di chi falsifica, altera o sopprime il contenuto delle stesse (artt. 617 *quater*, *quinques* e *sexties* c.p.)[82]. In tal modo, si è inteso tutelare penalmente le comunicazioni elettroniche al pari di quelle telefoniche e telegrafiche, che altrimenti sarebbero rimaste prive di garanzie.

Analogamente, è stata punita anche la condotta di chi accede abusivamente ad un sistema informatico altrui[83], inserendo un nuovo articolo (615 *ter*) nella sezione del codice penale dedicata ai delitti contro l'inviolabilità del domicilio ed inducendo parte della dottrina e della stessa giurisprudenza di legittimità a configurare l'esistenza di un nuovo tipo di 'luogo': il *domicilio informatico*[84]. La condotta di chi, ad esempio, tramite la rete Internet riesce ad accedere alle risorse di un computer remoto[85]

---

rilevanza economica dei dati personali V. CARIDI, *La tutela dei dati personali in Internet: la questione dei logs e dei cookies alla luce delle dinamiche economiche dei dati personali*, cit., 767 ss.; D. FONDAROLI, *La tutela penale dei « beni informatici »*, in questa *Rivista*, 1996, 302 ss.

[79] V. FROSINI, *La criminalità informatica*, in questa *Rivista*, 1997, 487; L. CUOMO-B. IZZI, *Misure di sicurezza e accesso abusivo ad un sistema informatico*, *cit. loc. cit.*

[80] In merito cfr. anche la disciplina apprestata dalla normativa comunitaria la quale prevede espressamente che gli Stati garantiscano la riservatezza delle comunicazioni elettroniche vietando l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o sorveglianza delle comunicazioni ad opera di persone diverse dagli utenti (art. 15, Direttiva 58/2002/CE, su cui *infra* parr. 8, 8.1, 8.2.).

[81] Trattasi della legge 23 dicembre 1993, n. 547 (in G.U. 30/12/1993, n. 305) intitolata « Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica ».

[82] Il problema dei reati informatici è particolarmente attuale coinvolgendo attività fra loro molto diverse: da quella di chi diffonde *virus* e altri programmi dannosi per il funzionamento del PC al fenomeno di chi, per gioco o dietro pagamento intercetta messaggi altrui o riesce ad introdursi nei sistemi informatici protetti (i cc.dd. *hackers* e *crackers*).

[83] L'art. 615 *ter* c.p. punisce espressamente « chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo »

[84] Così Cass. pen., sez. V, 7 novembre 2000, n. 12732, in *Cass. pen.*, 2002, 1015, con nota di L. CUOMO-B. IZZI, *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico*, *ivi*, 1018 ss.; Cass. pen., sez. VI, 4/10/1999, n. 3067, in *Cass. pen.*, 2000, 2990, con nota di A. ATERNO, *Sull'accesso abusivo a un sistema informatico*, *ivi*, 2994 ss., L. CUOMO, *La tutela penale del domicilio informatico*, *ivi*, 2998 ss.; Cass. pen., sez. VI, 4/10/1999, n. 3065, in *Riv. pen.*, 2000, 226; Trib. Torino, 7/02/1998, in *Giur. mer.*, 1998, 708, con nota di M. NUNZIATA, *La prima applicazione giurisprudenziale del delitto di « accesso abusivo ad un sistema informatico » ex art. 615* ter *c.p.*, *ivi*, 711. Alcuni autori, al contrario, non hanno ritenuto corretta la collocazione sistematica della disposizione citata, dubitando dell'esistenza di un domicilio informatico; cfr. R. BIN-F. PITRUZZELLA, *Diritto costituzionale*, Torino, 2003, 483.

di un altro utente[86] — a sua insaputa e contro la sua, espressa o tacita, volontà — è equiparata a quella di chi si introduce nel domicilio materiale della persona, anche se è chiaro che non potrà trattarsi di un accesso fisico ma meramente « logico »[87].

Probabilmente, il motivo che ha spinto il legislatore ad assegnare al reato di accesso abusivo a sistema informatico la particolare collocazione sistematica risiede nella identità di *ratio* che ispira anche le altre disposizioni penali poste a tutela del domicilio della persona: la volontà di tutelare la libertà del singolo vietando qualsiasi intromissione o interferenza nella sfera privata del soggetto[88].

La scelta parlamentare, che accoglie un concetto di domicilio particolarmente ampio ed originale, induce, in primo luogo, ad interrogarsi in merito alla possibilità di assegnare, anche a livello costituzionale, una nuova dimensione al luogo tutelato dall'art. 14 Cost. non più legata alla fisicità dello spazio.

È noto come non esista un'unica nozione di domicilio che assume invece diversi significati nel diritto civile, penale o fiscale[89]. Ai fini civilistici, ad esempio, esso è il luogo in cui una persona ha stabilito la sede principale dei suoi affari e interessi (art. 43 c.c.), mentre nelle disposizioni del codice penale diventa l'*abitazione* e ogni « *altro luogo di privata dimora* », nonché le « *appartenenze di essi* » (art. 614 c.p.).

Se è pacifico che il domicilio di cui all'art. 14 Cost. non si riduca alla nozione di cui all'art. 43 c.c.[90], più controverso è se esso rappresenti un mero riconoscimento della definizione della norma penalistica[91], per cui la disposizione costituzionale identificherebbe — secondo un'interpretazione estensiva — « qualunque luogo nel quale la persona abbia diritto di rinchiudersi, sulla base di un qualsiasi titolo giuridico [...] per condurvi la propria vita privata, per coltivare gli affetti, i propri interessi culturali,

---

85 'Remoto' nel linguaggio informatico è un temine utilizzato per indicare il computer, o anche la risorsa, posto a distanza dal sistema centrale di elaborazione.

86 Ma il discorso potrebbe essere lo stesso anche nel caso in cui si accedesse *off-line* al contenuto della memoria di un processore contro la volontà del proprietario.

87 L. Cuomo-B. Izzi, *Misure di sicurezza e accesso abusivo ad un sistema informatico*, cit., 1020-1021, i quali precisano che, nel caso della violazione del sistema informatico, si tratterebbe di un « accesso alla conoscenza », ossia dell'acquisizione materiale dei dati memorizzati nel sistema (Così D. Lusitano, *In tema di accesso abusivo a sistemi informatici o telematici*, in *Giur. it.*, 1998, 1924).

88 D. Lusitano, *In tema di accesso abusivo a sistemi informatici o telematici*, *cit. loc. cit.* Sul punto cfr. anche Trib. Torino, 7/2/1998, cit., il quale ritiene che la norma di cui all'art. 615 *ter* c.p. sia una estensione della protezione penale offerta al domicilio « reprimendosi qualsiasi introduzione in un sistema informatico che avvenga contro la precisa volontà dell'avente diritto ». Cfr. anche Cass. pen., sez. V, 7 novembre 2000, n. 12732; Cass. pen., sez. VI, 4/10/1999, n. 3065.

89 A. Barbera, F. Cocozza, G. Corso, *Le situazioni soggettive. Le libertà dei singoli e delle formazioni sociali. Il principio d'eguaglianza*, in G. Amato-A. Barbera (a cura di), *Manuale di diritto pubblico*, I, Bologna, 1984, 268.

90 T. Martines, *Diritto costituzionale*, Milano, 2000, 653.

91 Nel senso che la nozione contenuta nell'art. 14 Cost. non introdurrebbe una nuova tipologia ma darebbe dignità costituzionale al concetto penalistico di domicilio A. Barbera, F. Cocozza, G. Corso, *Le situazioni soggettive. Le libertà dei singoli e delle formazioni sociali. Il principio d'eguaglianza*, cit., 268. sul punto cfr. anche R. Bin-F. Pitruzzella, *Diritto costituzionale*, cit., 483.

artistici, sociali, politici, ma anche per svolgere la propria attività professionale o economica »[92].

Parte della dottrina ritiene che non vi sarebbe una necessaria coincidenza fra l'ambito di applicazione della norma penale e quella costituzionale. Quest'ultima potrebbe favorire una dimensione del domicilio anche più ampia rispetto a quello penale ed, a sua volta, il legislatore « potrebbe tutelare sotto la rubrica inviolabilità del domicilio anche la proprietà o altri diritti patrimoniali su cose mobili o immobili »[93] che non ricadono nel concetto di cui all'art. 14 Cost.

Si vuole, tuttavia, tentare di capire se la norma costituzionale non possa essere suscettibile di una diversa esegesi in ragione dell'evoluzione delle nuove tecnologie informatiche.

L'art. 14 Cost. deve essere interpretato alla luce del contesto logico-sistematico in cui si inserisce ed in combinato disposto con gli enunciati contenuti negli artt. 13 e 15 Cost. con cui risulta accomunato dalla tutela del medesimo valore fondamentale: preservare i cittadini da indebite interferenze altrui[94]. In tale contesto, vi sarebbe un unico filo conduttore fra tutela della libertà personale e tutela del domicilio per cui « il fondamento dell'inviolabilità domiciliare sarebbe la *riservatezza* piuttosto che la proprietà dei beni », con la conseguenza che « la norma costituzionale tutelerebbe la persona e non i luoghi »[95].

In ragione di queste considerazioni, il concetto di domicilio ai sensi dell'art. 14 Cost. può essere inteso in maniera particolarmente ampia esprimendo quella che è stata definita la « proiezione spaziale della persona »[96], ed identificandosi con « quello spazio isolato dall'ambiente esterno legittimamente ed attualmente adibito allo svolgimento delle mansioni della vita e dal quale il soggetto o i soggetti titolari intendano normalmente escludere la presenza di terzi »[97].

La stessa Corte Costituzionale, inoltre, ha mostrato di preferire una concezione di domicilio particolarmente avanzata comprendendovi « qualsiasi spazio isolato dall'ambiente esterno di cui il privato disponga legittimamente »[98].

Il vero problema, tuttavia, è capire se l'ambiente dal quale la persona ha il diritto di escludere gli altri debba essere necessariamente un luogo fisico o possa essere anche uno spazio immateriale (*i.e.* 'virtuale').

In effetti, pensando al tipo e alla quantità di informazioni che possono risiedere nella memoria di un qualsiasi processore — banche dati, lavori

---

92 A. Barbera, F. Cocozza, G. Corso, *op. cit. loc. cit.*

93 A. Pace, *Problematica delle libertà costituzionali*, cit., 218, nota 6.

94 Sulla stretta connessione fra le disposizioni contenute negli artt. 13, 14 e 15 Cost. cfr. Corte cost., 24/4/2002, n. 135.

95 A. Pace, *op. cit.*, 218 riprendendo le opinioni espresse dalla giurisprudenza statunitense *ivi* citata (corsivo nostro).

96 A. Amorth, *La Costituzione italiana. Commento sistematico*, Milano, 1948, 62 citato anche da P. Barile, *Istituzioni di diritto pubblico*, Padova, 1995, 645 e da A. Pace, *op. cit. loc. cit.*

97 P. Barile, *Istituzioni di diritto pubblico*, *cit. loc. cit.*

98 Cfr. Corte Cost. sent. 31/3/87 n. 88, con la quale si è ritenuto che anche il bagagliaio di un automobile rientrasse nella nozione di domicilio di cui all'art. 14 Cost. *Contra* A. Pace, *op. cit.*, 215, il quale ritiene che l'automobile non possa essere considerata domicilio in quanto, servendo a circolare, la sua tutela rientrerebbe in quella della libertà personale.

professionali, dati personali — oppure alle attività che si possono svolgere con un computer — ricercare, dialogare con altri soggetti, navigare in rete — il sistema informatico finisce con l'acquisire una dimensione propria ed indipendente dal mondo fisico che lo circonda. Ecco perché, proprio da questo punto di vista, ben potrebbe essere considerato come una sorta di « proiezione ideale »[99] di quello spazio di pertinenza della persona tutelato dal domicilio costituzionale cui, di conseguenza, dovrebbe estendersi lo stesso *jus excludendi alios*.

Non sorprende, allora, che il legislatore ordinario, con l'art 615 *ter* c.p., abbia voluto garantire i sistemi informatici alla stregua del domicilio tradizionale. Il valore tutelato, infatti, non appare diverso da quello garantito dall'art. 14 Cost. bensì una sua diretta attuazione.

5. Il valore economico delle informazioni registrate via internet e le modalità tecniche per creare un esatto profilo sociale dell'utente telematico.

Il progressivo aumento e sviluppo dei servizi *web* ha provocato una forte crescita della quantità e della qualità delle informazioni diffuse, creando l'esigenza di apprestare una maggiore tutela per la riservatezza e l'identità personale del singolo. In Internet l'acquisizione e lo scambio della 'conoscenza' avviene contemporaneamente a quello di dati personali[100] e sociali[101] del navigatore, a volte anche a sua insaputa, secondo determinati meccanismi che si analizzeranno nel prosieguo della trattazione.

La navigazione nel *web* comporta, infatti, la possibilità di registrare innumerevoli informazioni riguardanti gli utenti conservate a vario titolo dagli operatori Internet. Nonostante un comune fraintendimento, infatti, chi naviga in rete non è realmente anonimo e, salvo l'utilizzo di particolari modalità[102] o accorgimenti tecnici[103], è sempre possibile risalire al soggetto titolare della linea da cui ci si connette[104].

[99] L. Cuomo-B. Izzi, *Misure di sicurezza e accesso abusivo ad un sistema informatico*, cit., 1019. Sul punto anche D. Lusitano, *In tema di accesso abusivo a sistemi informatici o telematici*, cit., 1924, il quale sottolinea come i delitti contro l'inviolabilità del domicilio sarebbero accomunati dalla « tutela della libertà, sotto l'aspetto del divieto di intromissioni, interferenze, turbative della sfera privata di un soggetto, che avvengano contro la volontà dello stesso » ecco perché il domicilio informatico può ben essere inteso come « l'ideale espansione del domicilio tradizionale ».

[100] In questo caso per dato personale si intende quello idoneo ad identificare anagraficamente il soggetto.

[101] Per dato sociale si intende quello idoneo ad identificare le abitudini ed i gusti del soggetto.

[102] Per esempio collegandosi da postazioni pubbliche in cui non vengono presi i dati identificativi degli utenti.

[103] Ci si riferisce all'utilizzo di *proxy server* o all'impiego di *software* particolari che consentono di generare falsi numeri IP.

[104] Ritiene che l'anonimato in Internet costituisca un valore da difendere S. Rodotà, *Proprietà, Privacy e Pornografia, le tre « P » di Internet*, in *Problemi dell'informazione*, 2-3, 2001, 239. Sul problema dell'anonimato in Internet e delle responsabilità in Rete D. Petrini, *La responsabilità penale per i reati via Internet*, Napoli, 2004, 76 ss.; G. Riccio, *Anonimato e responsabilità in Internet*, in questa *Rivista*, 2000, 314 ss.

Nel mondo fisico si può camminare per strada, entrare in un negozio, comprare un giornale senza che necessariamente commessi e proprietari identifichino il singolo, registrino quante volte sia entrato nel proprio magazzino, cosa abbia visto o comprato; nel mondo virtuale tutto questo in sostanza non accade quasi mai. Ciò è dovuto non tanto al funzionamento tecnico della rete, quanto alla circostanza che le informazioni personali e quelle riguardanti le abitudini sociali della persona costituiscono un'enorme risorsa economica[105] per gli operatori telematici con cui, nella maggior parte dei casi, si riesce a finanziare il funzionamento di tutta una serie di servizi offerti attraverso la rete *apparentemente* gratuiti.

Come è stato efficacemente sottolineato « le nuove tecnologie dovrebbero essere chiamate 'tecnologie relazionali' o *R-technologies*, e non più tecnologie informatiche »[106], perché grazie ai nuovi programmi per elaboratore è possibile « stabilire reticoli complessi di interconnessioni e di relazioni fra fornitori e utenti, creando l'opportunità di quantificare e trasformare in merce, sotto forma di relazioni economiche a lungo termine, ogni aspetto dell'esperienza di vita di ciascuno »[107].

La rete, quindi finisce per essere utilizzata come una preziosissima « fonte di approvvigionamento »[108] di dati personali, perché consente di registrare le informazioni riguardanti la vita dei soggetti della natura più disparata. Il *World Wide Web* si trasforma così in una vera e propria tecnica di sorveglianza[109] divenendo « uno dei più rapidi mezzi di sviluppo del marketing commerciale »[110].

I dati degli utenti raccolti *on-line*, infatti, dopo essere stati memorizzati — nella maggior parte delle ipotesi — sono elaborati allo scopo di creare dei profili più o meno dettagliati dei navigatori[111]; in seguito, vengono ri-

---

[105] Le informazioni riguardanti gusti, abitudini e interessi consentono di creare dei veri e propri 'profili' dell'individuo aventi un vero e proprio valore economico tanto da costituire una « nuova ''merce'' » (S. Rodotà. *Tecnologie e diritti*, cit., 66, 81, 110). Sul punto anche V. Caridi, *op. cit.*, 768 e nt. 15 che precisa come: « Le notizie idonee ad identificare un soggetto, dalle più semplici e scarne quali quelle anagrafiche, a quelle che ne delineano il profilo come consumatore, quali attitudini al consumo, gusti e capacità reddituale, sino a quelle più intime e personali, quali quelle attinenti alla salute ed alle attitudini sessuali o alle opinioni politiche e religiose, divengono oggetto di raccolta, di selezione, di aggregazione e di stoccaggio in banche dati. Il fine è quello di arrivare ad un profilo del consumatore-utente quanto più completo possibile ed in ogni caso tale da offrirgli proprio il prodotto o il servizio che egli è più propenso ad acquistare » (p. 768).

[106] J. Rifkin, *L'era dell'accesso*, trad. it. P. Canton, Milano, 2001, 131.

[107] J. Rifkin, *L'era dell'accesso*, cit., 136, che in seguito precisa come « Nella vecchia economia industriale, la forza lavoro di ogni individuo è considerata una forma di proprietà esclusiva che può essere venduta sul mercato. Nella *new economy*, la cessione dell'accesso allo stile di vita e alle esperienze esistenziali di un individuo, espressi dalle sue decisioni di acquisto, è un patrimonio intangibile di uguale rilevanza e altrettanto ricercato » (pp. 137 e 138).

[108] V. Caridi, *op. cit.*, 769.

[109] D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, cit., 139, che sostiene: « I database impiegati nel marketing fanno esplicitamente parte di ciò che ho definito ''il world wide web di sorveglianza''. L'espressione è metaforica e comprende qualunque forma di sorveglianza che si esprima nel cyberspazio o attraverso comunicazioni mediate dal computer. Ogni impiego di Internet, il world wide web e i sistemi di posta elettronica sono tracciabili e questa possibilità è stata rapidamente sfruttata dal momento che i media in questione sono commercializzati ».

[110] D. Lyon, *ult. op. cit.*, 123

[111] G. Maccaboni, *La profilazione dell'utente telematico fra tecniche pubblicita-*

venduti a società pubblicitarie le quali li utilizzano per personalizzare sempre di più i propri messaggi promozionali[112]. Se si escludono i siti a pagamento, il *marketing* diretto è la principale fonte di guadagno dei fornitori di accesso e di servizi telematici[113].

Internet si trasforma, in tal modo, in un vero e proprio 'mercato' di dati personali dalle caratteristiche però del tutto anomale perché ad una precisa « domanda » non corrisponde una « offerta » veramente consapevole. Nella maggior parte dei casi, infatti, l'utente non sa di stare cedendo « un prodotto avente valore economico »[114].

Molto variegate sono le tipologie di dati prelevati e conservati dai diversi attori della rete[115] nonché le relative modalità di acquisizione. In alcuni casi, come si vedrà, si tratta, oltretutto, di informazioni registrate per *default* ossia in modo automatico in base alle impostazioni del *software* di navigazione o attraverso determinati programmi registrati sul computer dell'utente, con la conseguenza che non ci si accorge — ed il più delle volte non si sa neanche — della loro registrazione.

L'operatore di telecomunicazione, ossia il proprietario dell'infrastruttura su cui viaggia il segnale[116], conserva le informazioni riguardanti il

rie online e tutela della privacy, in questa *Rivista*, 2001, 425 ss.

[112] Sul punto si rimanda alle precisazioni di D. Lyon, *La società sorvegliata*, cit., 139, che, in proposito, spiega come « I database utilizzati nel marketing operano come una tecnologia selettiva » attraverso la quale « [...] i consumatori sono selezionati e guidati sulla base di informazioni personali assunte sia da fonti pubbliche, sia da registrazioni dirette del comportamento del consumatore ».

[113] Ad esempio, molti motori di ricerca — fra cui lo stesso *Google* — sono finanziati esclusivamente dalla pubblicità ospitata sul sito. Cfr. sul punto anche G. Arnò-A. Lensi Orlando, *La tutela della privacy nella rete Internet*, Torino, 2002, 59, che precisano come: « Il fatto che i dati personali degli utenti costituiscono un vero e proprio patrimonio ed abbiano un valore economico ben individuabile è confermato dalla circostanza che molte imprese attive nel settore dell'*e-commerce* e delle telecomunicazioni offrano servizi gratuiti ai consumatori che comunichino i propri dati personali. [...] Tali imprese erano ben consce del valore dei dati che ricevevano e dell'utilizzo che ne potevano fare, ed offrivano in cambio della loro comunicazione una serie di servizi la cui quantità e qualità era calcolata in funzione di un preciso ''tasso di conversione'' da esse stesso individuato » (in part. p. 59, nt. 8).

[114] V. Caridi, *op. cit.*, 769. L'A. sostiene in proposito che, quando si rivelano i propri dati per accedere ad un determinato servizio compilando appositi questionari — come ad esempio un *guestbook* — oppure, nei casi in cui si forniscono dati inconsapevolmente — attraverso l'utilizzo di *cookies* di cui si dirà —, coloro che cedono le proprie informazioni non potrebbero essere considerati come dei veri e propri 'offerenti' poiché « non può individuarsi una 'domanda' nelle tecniche più o meno lecite di raccolta del prodotto ''dato personale''. Si tratterebbe, secondo la dottrina che si riporta, di un « mercato falsato » in quanto « la circolazione del prodotto avviene sulla base delle sole esigenze di una parte e non in base al suo fisiologico funzionamento che prevede, invece, il libero e cosciente confronto dei protagonisti della domanda e dell'offerta ». La tesi, invero, era già stata sostenuta da S. Rodotà, *Tecnologie e diritti*, cit., 55, 82-83; che ha evidenziato, in proposito, come il consumatore si troverebbe in una posizione di « disparità » nei confronti del fornitore di servizi telematici e informatici per cui si potrebbe anche dubitare della esistenza di un « consenso liberamente formato » (p. 55).

[115] La classificazione delle categorie di dati prelevati attraverso la rete Internet che si offre nel testo si avvale dei risultati del documento di lavoro adottato il 21 novembre 2000 dal « Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali » istituito *ex* art 29 della direttiva comunitaria 95/46/CE, 5063/00/IT/DEF, WP 37, pp. 11, 12, consultabile nel sito *www.garanteprivacy.it*, cui si rinvia per un'analisi più approfondita dell'argomento.

[116] Rientrano in tale categoria società

traffico, essenzialmente a fini di fatturazione, alla stregua di quanto avviene per le comunicazioni telefoniche. I soggetti rientranti in questa categoria registrano, quindi, il numero delle chiamate — per i telefoni cellulari anche la localizzazione — la data, l'ora e la durata del collegamento.

Il fornitore di accesso Internet[117], ossia l'operatore con il quale si stipula l'abbonamento per poter accedere alla rete[118], conserva i dati anagrafici — nome, indirizzo, e altri dati personali diversi a seconda dell'operatore scelto (data di nascita, sesso, gusti ecc.) — il nome di identificazione (*user-id*) e la password di accesso. Tale soggetto, inoltre, registra sempre il numero di identificazione del computer[119], la data e l'ora di connessione in appositi *files* riservandosi la possibilità di individuare l'utente telematico.

I fornitori di servizi Internet[120], ossia coloro che offrono ospitalità a pagine *web*, danno accesso a gruppi di discussione, forniscono caselle di posta elettronica[121], creano automaticamente un registro in cui possono conservare più o meno tutto ciò che accade sul proprio sito. In tal modo, memorizzano non solo l'indirizzo IP dell'utente che desidera accedere e i dati presenti nell'intestazione di richiesta *http*[122], ma anche la data, l'ora e la durata della connessione, nonché ad esempio, le parole chiavi inserite nel sito per effettuare una ricerca, i *link*[123] visitati o i *banner*[124] aperti.

Va anche considerato che nella realtà non vi è sempre una distinzione fisica fra le tre categorie di operatori descritti, per cui spesso i fornitori di accesso sono anche fornitori di servizi ed il proprietario dell'infrastruttura può anche dare accesso alla rete o fornire determinate risorse via Internet. Di conseguenza, le informazioni descritte possono anche essere con-

---

ad esempio come Telecom, Vodafone, Wind, *etc*.

[117] Anche chiamato *Internet access provider*.

[118] Si tratta di un abbonamento — per le connessioni analogiche solitamente gratuito — con soggetti presso cui ci si registra — tra i più comuni, fra quelli italiani: Libero, Virgilio etc. — e che offrono anche tutta una serie di servizi *web* come la posta elettronica o la possibilità di accedere a notizie, *forum*, *etc*.

[119] È il cosiddetto indirizzo IP (acronimo per *Internet protocol*) ossia il numero che consente di identificare ogni computer connesso alla rete. Quando, ad esempio, si desidera visualizzare una determinata pagina *web*, il server sul quale risiedono materialmente le informazioni ricercate invierà i dati relativi all'elaboratore richiedente attraverso il numero di identificazione che gli ha assegnato il fornitore di accesso Internet. Il numero IP funziona proprio come se fosse un indirizzo, o meglio un numero di telefono, al quale vengono di volta in volta inviati i dati richiesti.

[120] Detti anche *Internet content provider o Internet service provider* (ISP).

[121] Trattasi di una categoria particolarmente ampia poiché in teoria chiunque può offrire un qualsiasi servizio sul *web* se titolare di un dominio, ossia « affitta[ndo] una connessione TCP/IP permanente e utilizza[ndo] *server* connessi permanentemente ad Internet » (la definizione è presa dalla relazione del « Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali » istituito *ex* art. 29, direttiva 95/46/CE, 21/11/2000, cit., p. 12).

[122] Tali sarebbero — a seconda del programma di navigazione installato — l'indirizzo della pagina richiesta, il numero di identificazione del computer, il tipo e la versione di *browser* installato, i programmi che leggono i formati installati, la lingua dell'utente. Non tutti i dati elencati sono funzionali ai fini della connessione e della navigazione, ma vengono comunque registrati dai fornitori di servizi *web*. Cfr. documento di lavoro 21/11/2000 del « Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali », cit., p. 16.

[123] Si tratta dei collegamenti ipertestuali che consentono di accedere ad altre pagine del sito oppure a siti diversi.

[124] Si tratta delle finestre pubblicitarie che si aprono all'interno delle pagine *web*.

frontate fra loro determinando rischi ancora maggiori per la riservatezza e l'identità personale dell'individuo, le cui abitudini sociali potrebbero essere tenute costantemente sotto controllo dai fornitori di servizi telematici 'potenzialmente' in grado di creare veri e propri *identikit* dei soggetti connessi alla rete conoscendone gli orari di collegamento, le pagine visitate e di conseguenza i gusti e le inclinazioni personali.

Dovrà analizzarsi, allora, l'applicabilità alla nuova società dell'informazione della vigente disciplina sulla protezione dei dati personali allo scopo di verificare se il grado di tutela apprestato sia rispettoso dei principi costituzionali posti a garanzia della persona e della sua 'riservatezza'.

6. La protezione dei dati personali fra diritto interno e diritto comunitario. La normativa applicabile ad Internet in attesa dell'approvazione del codice di deontologia dei fornitori di comunicazioni e informazioni.

Il diritto alla protezione dei dati personali è espressamente riconosciuto, nel nostro ordinamento, dall'art. 1 del Decreto legislativo 30 giugno 2003, n. 196 (d'ora in poi ''codice in materia di protezione dei dati personali'' o ''codice sulla *privacy*'') che recepisce totalmente il contenuto dell'art. 8 della Carta europea dei diritti fondamentali[125].

Il codice, che abroga la precedente disciplina in materia, ha l'indubbio merito di ricondurre a sistema la frammentata normativa italiana sulla protezione dei dati personali. Esso costituisce, infatti, l'ultima tappa di un *iter* normativo cominciato con la legge 675/96 — e successive modifiche — poi continuato con l'emanazione del decreto legislativo 171/98, contenente specifiche disposizioni per la vita privata nel settore delle telecomunicazioni. La normativa italiana ha recepito, in tal modo, le direttive comunitarie 95/46, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, e 97/66 che traduceva i principi già enunciati in specifiche norme per il settore delle telecomunicazioni.

È, tuttavia, noto come l'affermazione dei nuovi sistemi di comunicazione integrata (etere, satellite, internet, digitale terrestre ecc.), ha condotto al superamento del tradizionale concetto di 'telecomunicazione' e la Comunità europea — adeguandosi alle nuove tecniche di trasmissione — ha approvato una nuova normativa con cui apprestare una tutela generale dei dati personali e della vita privata per tutte le ''comunicazioni elettroniche'' accessibili al pubblico, indipendentemente dalle tecnologie utilizzate. Il riferimento è alla Direttiva 58/2002 del Parlamento e del Consiglio del 12 luglio 2002[126] — recentemente modificata dalla direttiva 2006/24/CE[127] — con cui è stata abrogata la precedente direttiva 97/66 che, elaborata per

[125] Sul significato del riconoscimento di un 'diritto alla protezione dei dati personali' G.P. Cirillo, *Disposizioni generali*, in Id. (a cura di), *Il codice sulla protezione dei dati personali*, Milano, 2004, 3 ss.; C. Filippi, *Principi generali*, in G.P. Cirillo (a cura di), *Il codice sulla protezione dei dati personali*, cit., 11 ss.; V. Italia, *Considerazioni sulla Rubrica dei Titolo I: « Principi generali »*, in Aa.Vv., *Codice della privacy*, tomo II, Milano, 2004, 18.

[126] Direttiva CE 12/07/2002 n. 58, in G.U.C.E. 31/07/2002 n. 201.

[127] Direttiva CE 15/03/2006 n. 24, in G.U.C.E. 13/04/2006 n. 105.

il settore della telefonia, era evidentemente inadatta alla regolazione delle nuove forme di trasmissione e di comunicazione, tra cui anche Internet[128].

Per il tema che qui interessa, appare significativo che il codice per la protezione dei dati personali — che, tra l'altro, recepisce anche la direttiva 58/2002 citata — abbia previsto, a differenza dei precedenti testi normativi, un apposito articolo dedicato ad Internet ed alle reti telematiche il quale rimanda però, per la specifica disciplina, all'autoregolamentazione degli stessi fornitori di servizi di comunicazione e di informazione. È, infatti, compito del Garante promuovere in materia l'elaborazione di un codice di deontologia e buona condotta in modo che venga 'assicurata' e 'uniformata' « una più adeguata informazione e consapevolezza degli utenti delle reti di comunicazione elettronica gestite da soggetti pubblici e privati rispetto ai tipi di dati personali trattati e alle modalità del loro trattamento » (art. 133)[129].

La soluzione è per molti versi simile a quella adottata nell'ordinamento americano dove il problema della protezione dei dati personali è rimandato all'autoregolamentazione degli stessi soggetti e gestori che acquisiscono le informazioni lasciando che sia alla fine il mercato a determinare il livello di protezione della *privacy* degli utenti[130], anche se, a differenza del caso citato, nell'esperienza italiana la funzione dei codici di deontologia è quella di implementare una disciplina generale già esistente in materia di trattamento dei dati personali nel settore delle comunicazioni elettroniche[131].

La ragione che ha spinto a rimandare le problematiche della tutela della riservatezza in Internet all'autodisciplina dei fornitori di servizi di comunicazione deriva indubbiamente anche da motivi tecnici e dalla difficoltà di stare continuamente al passo con le rapide evoluzioni delle nuove tecnologie di informazione[132]. Il carattere maggiormente flessibile dei codici di

---

[128] A. Pradella, *Comunicazioni elettroniche*, in G.P. Cirillo (a cura di), *Il codice sulla protezione dei dati personali*, cit., 442.

[129] Il legislatore ha indicato, in proposito, quali devono essere le modalità per la raccolta dei dati in rete precisando la necessità di fornite l'informativa *online* in modo « agevole e interattivo » per assicurare « una più ampia trasparenza e correttezza » nei confronti degli utenti nonché il rispetto dei principi di liceità, correttezza, esattezza, pertinenza che valgono in generale, *ex* art. 11 del codice del 2003, per tutti i trattamenti di dati.

[130] Cfr. quanto considerato *supra* in par. 1 e note 16, 17.

[131] L'art. 12 del d.lgs. 196/03 prevede, infatti, che, in alcuni settori, l'Autorità garante possa incentivare l'autoregolamentazione e vigilare sulla conformità alle leggi ed ai regolamenti vigenti dei codici elaborati. Sul problema della tutela dei dati personali e della tendenza delle imprese private ad adottare codici di autoregolamentazione in materia, si rimanda alle considerazioni di S. Rodotà, *Tecnologie e diritti*, cit., 56 ss. Sul tema cfr. anche M. Cartabia, *Le norme sulla* privacy *come osservatorio sulle tendenze attuali delle fonti del diritto*, in G.M. Losano (a cura di), *La legge italiana sulla* privacy. *Un bilancio dei primi cinque anni*, Bari, 2001, 61; G. Pino, *I codici di deontologia nella normativa su trattamento dei dati personali*, in *Danno e responsabilità*, 2002, 363; A. Simoncini, *I codici deontologici di protezione dei dati personali nel sistema delle fonti: l'emersione di un nuovo « paradigma » normativo?*, in U. De Siervo (a cura di), *Osservatorio sulle fonti 1999*, Torino, 2000, 284. Per un commento all'attuale art. 12 del codice per la protezione dei dati personali vd. H. Simonetti, *Codici di deontologia e buona condotta*, in G.P. Cirillo (a cura di), *Il codice sulla protezione dei dati personali*, cit., 55 ss.

[132] Cfr. *Relazione per l'anno 2003* dell'Autorità garante per la protezione dei dati personali p. 90, in *www.garanteprivacy.it*. Dal punto di vista dei soggetti economici, invece, l'esigenza di autoregola-

autoregolamentazione li renderebbe, infatti, degli strumenti di regolamentazione più congeniali alla realtà cui si riferiscono[133].

Il rispetto del codice di deontologia di cui all'art. 133, d.lgs. 96/33, costituisce condizione di liceità per il trattamento dei dati degli utenti in Internet[134] e la creazione di *standards* di protezione uniformi, infatti, dovrebbe comunque riuscire a creare una maggiore informazione e consapevolezza negli utenti telematici sulla politica adottata in materia di *privacy* dai siti visitati. La normativa vigente sancisce, infatti, che le norme deontologiche prevedano anche la possibilità di rilasciare « certificazioni attestanti la qualità delle modalità prescelte e il livello di sicurezza assicurato »[135] a chi garantisca — attraverso una informativa rispettosa dei principi contenti nell'art. 13, d.lgs. 196/03 — la più ampia trasparenza e correttezza nei confronti degli utenti. In tal modo, sarebbe più facile e veloce l'individuazione del grado di protezione della riservatezza apprestato dai siti, ed i navigatori telematici potrebbero riservarsi la possibilità di decidere se visitare determinate pagine *web* proprio sulla base della presenza o meno di quella certificazione che garantisce l'esistenza di un determinato *standard* di tutela della propria riservatezza.

Ciononostante rimane il fatto che, a più di tre anni dall'entrata in vigore del d.lgs. 196/03 il codice di deontologia previsto dall'art. 133 sia ancora in fase di preparazione lasciando inattuata l'unica specifica disposizione su Internet e sulle reti telematiche cui non resterà che applicare le altre disposizioni del codice per la protezione dei dati personali in quanto compatibili.

In proposito, si può affermare con un buon grado certezza che, alla raccolta ed al trattamento delle informazioni acquisite attraverso la rete, si estendano i principi che informano il decreto legislativo del 2003 (artt. 1-9) e le disposizioni generali che — recependo la direttiva quadro 95/46/CE ed abrogando la legge 675/96 — si applicano a tutti i trattamenti di dati indipendentemente dal mezzo utilizzato (artt. 11-45).

Il codice sulla *privacy*, inoltre, appresta una specifica ed uniforme disciplina per il trattamento dei dati personali « connessi alla fornitura di servizi di comunicazioni elettronica accessibili al pubblico su reti pubbliche di comunicazione »[136]. Dalle definizioni fornite dallo stesso testo normativo

---

mentarsi nasce dal fatto che la raccolta delle informazioni personali è un elemento fondamentale per lo sviluppo della *net-economy* per cui « qualunque forzatura istituzionale ne limiterebbe lo sviluppo » (D. CALENDA, *Il dibattito internazionale sui limiti e le tendenze delle politiche per la tutela della privacy in Internet*, in *Riv. it. dir. pubb. com.*, 2001, 540, cfr. anche nt. 18).

[133] Sulla tendenza anche dell'ordinamento comunitario a spingere verso la promozione di codici di condotta destinati a contribuire alla corretta applicazione delle disposizioni nazionali in materia di protezione dei dati personali cfr. l'art. 27 della direttiva 95/46/CE, poi recepito nell'abrogata legge 675/96. Sul punto P. BILANCIA, *Attività normativa delle autorità indipendenti e sistema delle fonti*, in S. LABRIOLA (a cura di), *Le autorità indipendenti*, Milano, 2000, 165; H. SIMONETTI, *Codici di deontologia e buona condotta*, in G.P. CIRILLO (a cura di), *Il codice sulla protezione dei dati personali*, cit., 57; A RUDELLI, *Internet e reti telematiche*, in AA.VV., *Codice della privacy*, cit., 1694.

[134] Cfr. quanto sostiene il Garante per la *privacy* con generale riferimento per tutti i codici di deontologia in S. RODOTÀ, *Relazione per l'anno 2003*, cit., 6 (*paper*).

[135] D.lgs. 196/2003, art. 133, ultima alinea.

[136] D.lgs. 196/2003, art. 121, che recepisce la definizione di comunicazione elettronica contenuta nell'art. 2, lett. *d*) della direttiva comunitaria 58/2002.

di « comunicazione elettronica », di « servizio di comunicazione elettronica » e di « rete pubblica di comunicazione[137] è facilmente argomentabile l'applicazione della disciplina particolare dei servizi di comunicazione elettronica anche ai servizi forniti tramite Internet (artt. 121 e seguenti).

7. L'estensione della normativa vigente. La distinzione fra trattamento dei dati « a raccolta palese » ed « a raccolta occulta ».

I *principi* enunciati dal legislatore nazionale che devono informare il trattamento automatizzato — nel rispetto delle indicazioni comunitarie — tutelano, almeno in linea di massima, il diritto alla riservatezza dell'utente telematico consentendo la conservazione solo in determinati casi ed a certe condizioni, a garanzia del diritto all'identità individuale e della *libertà di scelta* del singolo in merito alla decisione di consentire o meno la comunicazione delle proprie informazioni personali.

Da questo punto di vista, è sancito, infatti, che la formazione di banche dati debba ispirarsi al ''principio di necessità'' nel senso che i sistemi informativi e i programmi informatici devono essere configurati in modo da ''ridurre al minimo'' le informazioni inerenti l'individuo. È, inoltre, specificato che, a tal uopo, il trattamento di « dati personali »[138] è consentito solo quando le finalità per cui gli stessi sono raccolti non possono ugualmente essere raggiunte tramite l'utilizzo di dati anonimi; mentre il trattamento dei « dati identificativi »[139] è consentito solo nel caso in cui siano previste « opportune modalità che permettano di identificare l'interessato solo in caso di necessità »[140]. Tutti i trattamenti di dati personali effettuati attraverso la rete Internet devono, inoltre, assicurare un « elevato grado di tutela » dei diritti e delle libertà fondamentali, nonché « della dignità dell'interessato »[141].

Necessità e dignità divengono in tal modo due parametri alla stregua dei quali valutare la liceità della costituzione di banche dati e della modalità di trattamento automatizzato delle informazioni personali raccolte. Questo significa che vi è un generale divieto alla costituzione di qualsivoglia banca dati lesiva del diritto degli utenti di decidere come e cosa della propria persona rendere disponibile a terzi. Tuttavia, tale diritto si affievolisce

---

[137] Cfr. d.lgs. 196/03, art. 4, co. 2, lett. *a*), *c*) e *d*).

[138] Ai sensi dell'art. 4, co. 1, lett. *b*), d.lgs. 196/2003, per dato personale si deve intendere « qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale ».

[139] Dati identificativi sono « i dati personali che permettono l'identificazione diretta dell'interessato » (art. 4, co. 1, lett. *c*), d.lgs. 196/2003).

[140] D.lgs. 196/2003, art. 3. Il principio di necessità costituirebbe quindi « un'ineludibile test legislativo per valutare la legittimità delle informazioni raccolte » (*Relazione* dell'Autorità garante per la *privacy* per l'anno 2003, cit., p. 5).

[141] D.lgs. 196/2003, art. 2: « Il presente testo unico, di seguito denominato codice, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali ».

quando non è possibile tecnicamente operare altrimenti — nel senso che senza la conoscenza del dato non è possibile effettuare la trasmissione della comunicazione — oppure nel caso di esigenze definite 'necessarie' e che si relazionano essenzialmente con ragioni di sicurezza pubblica di cui si dirà. In ogni caso, la conservazione effettuata deve rispettare diritti e dignità del singolo per cui, ad esempio, il trattamento sarà sicuramente illecito se congegnato in modo tale da poter ledere la rispettabilità, l'onorabilità, la stima dei soggetti cui appartengono le informazioni[142].

Se questi sono i principi generali cui si ispira il codice, bisogna analizzare se essi sono rispettati anche nelle ipotesi particolari.

Per quanto interessa questa sede, durante la navigazione in Internet bisogna in primo luogo distinguere fra dati personali acquisiti mediante un comportamento attivo dell'utente il quale rivela le proprie informazioni (dati cc.dd. « a raccolta palese ») e dati memorizzati dai singoli operatori della rete senza alcun tipo di collaborazione (dati cc.dd. « a raccolta occulta »)[143].

Nella prima categoria rientrano i dati forniti dalla persona che volontariamente si registra presso un operatore telematico allo scopo di usufruire di un particolare servizio. Le ipotesi sono numerose: la stipulazione dell'abbonamento per effettuare la connessione, l'utilizzo della posta elettronica, la partecipazione ad un *newsgroup*, a volte la stessa consultazione di una pagina *web* o lo 'scaricamento' di un *file*, la creazione di un sito e così via.

In tutti questi casi non si pongono particolari problemi di estensione della disciplina vigente in quanto sono applicabili le disposizioni generali previste per tutti i trattamenti di dati personali a prescindere dalla natura dello strumento tecnico utilizzato per la raccolta.

In tali ipotesi, è assicurata la libertà di scelta dell'utente, tutelando la sua riservatezza, in quanto è sempre necessaria la richiesta — previa informazione circa le finalità e le modalità del trattamento[144] — del consenso dell'interessato. Inoltre, anche in caso di approvazione, il singolo non perde ogni prerogativa sulle proprie informazioni, ma il suo diritto all'identità individuale è assicurato dal riconoscimento del diritto di accesso, rettifica e cancellazione come una sorta di « contrappeso »[145] alla parziale perdita di disponibilità dei propri dati.

Sotto il profilo descritto, l'acquisizione dei dati non pone problemi differenti rispetto a qualsiasi altro trattamento effettuato, anche senza l'utilizzo della rete internet, per cui in questa sede non si approfondiranno ulteriormente le relative questioni[146].

Più problematico è, invece, il caso di quelle informazioni raccolte in maniera invisibile durante la navigazione che ben potrebbero essere utilizzate

---

[142] Per un'analisi del significato del temine dignità si rimanda alle considerazioni contenute *supra* nei parr. 2 e 3.

[143] La distinzione fra dati a raccolta palese ed occulta si rinviene in G. Arnò-A. Lensi Orlando, *La tutela della privacy nella rete Internet*, cit., 51 ss.

[144] Sui problemi inerenti il contenuto dell'informativa si rinvia a G. Arnò-A. Lensi Orlando, *op. cit.*, 53 ss.

[145] A. Baldassare, *Privacy e Costituzione*, cit., 434. Stesso concetto è espresso anche da S. Rodotà, *Progresso tecnico e problemi istituzionali nella gestione delle informazioni*, cit., 31.

[146] In proposito, si rinvia alla bibliografia citata nelle note 46 e 47.

per fini sconosciuti all'utente, senza la possibilità di controllarne la circolazione[147]. Le tecniche — non necessariamente illecite — per l'acquisizione di tali dati sono diverse e non sottoponibili alla medesima disciplina giuridica per cui è necessario operare le opportune distinzioni.

8. Dati di traffico, file di *log* e tutela della riservatezza.

Una prima categoria di dati registrati 'passivamente' sono i cc.dd. dati di traffico ossia quelli inerenti la trasmissione della comunicazione. In tale categoria rientrano, quindi, le informazioni relative al momento e alla durata della connessione nonché ai numeri chiamati, che nel caso di Internet corrispondono ai numeri IP (*rectius* agli indirizzi *web*) dei siti consultati. Tali informazioni insieme ai dati anagrafici forniti dall'utente ed al numero di identificazione del computer possono consentire al soggetto titolare del trattamento di ricostruire le abitudini sociali dell'utente telematico del quale può sapere come, quando, quanto, per quante volte si connette abitualmente nonché quali siti ha visitato e con quale frequenza. Si può facilmente immaginare che, senza le opportune forme di garanzia, la sfera privata del navigatore telematico sarebbe completamente inesistente in palese violazione di quei valori contenuti nelle disposizioni costituzionali, di cui si è detto[148], che tutelano la privatezza e l'intimità dalle indebite intrusioni altrui.

In proposito, le regole applicabili sono state recentemente oggetto di modica da parte del legislatore nazionale e dovranno ulteriormente essere rivisitate alla luce nuove disposizioni contenute nella direttiva comunitaria 24/2006 relativa alla vita privata e alle comunicazioni elettroniche.

L'art. 123 del codice per la protezione dei dati personali, appresta una specifica disciplina per i dati relativi al traffico dei servizi di comunicazione elettronica fra i quali — stante la definizione normativa[149] — rientrerebbero anche i dati delle comunicazioni transitanti nel *web* registrati dai fornitori di accesso nei registri di connessione (file di *log*[150]) e nei « database relativi a codici identificativi ed anagrafici del cliente »[151].

---

147 G. Arnò-A. Lensi Orlando, *op. cit.*, 85, che sul punto richiama le parole del *Working Party*, raccomandazione n. 1/99 del 23/2/99 del Gruppo di lavoro sulla tutela dei dati personali, sul *Traffico invisibile ed automatico dei dati su Internet effettuato da software ed hardware* (consultabile in *www.garanteprivacy.it*).

148 Cfr. quanto osservato *supra* in par. 2.

149 Secondo l'art. 123 citato, « dato relativo al traffico » è « qualsiasi dato sottoposto al trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica e della relativa fatturazione ». La disposizione aggiorna l'abrogata legge 171/98 che, invece, prendeva in considerazione solo le informazioni necessarie per l'inoltro delle chiamate. Oggi la definizione tiene conto non solo dei servizi telefonici ma di tutte le comunicazioni elettroniche. In tal senso, A. Pradella, *Comunicazioni elettroniche*, cit., 447.

150 Sul concetto di '*data log*' e sul problema della loro conservazione C. Parodi, *I file di log*, in Id., *Le intercettazioni*, Torino, 2002, 70; G. Ciacci, *La tutela dei dati personali su Internet*, in A. Loiodice-G. Santaniello (a cura di), *La Tutela della riservatezza*, cit., 378; V. Caridi, *La tutela dei dati personali in Internet...*, cit., 771; E. Tosi, *Prime osservazioni sull'applicabilità della disciplina generale della tutela dei dati personali a Internet e al commercio elettronico*, in questa *Rivista*, 1999, 594; Id., *La tutela dei dati personali*, in Id., *I problemi giuridici di Internet*, Milano, 2001, 83.

151 A. Pradella, *op. cit. loc. cit.*, che richiama le parole di C. Filippi, *Il trattamento dei dati personali*, in F. Maschio (a

La disciplina richiamata stabilisce che tutte queste informazioni debbano essere cancellate o rese anonime una volta terminata la comunicazione salvo il caso che non siano necessarie ai fini della fatturazione o della contestazione del pagamento e per un periodo non superiore ai sei mesi.

Le regole descritte valgono per chi concede il servizio a pagamento come il proprietario dell'infrastruttura che consente di collegarsi alla rete il quale, in alcuni casi, è anche il fornitore del servizio telefonico. Di contro, non dovrebbero estendersi ai fornitori di accesso alla rete[152] se forniscono un abbonamento gratuito[153], in quanto non fatturano alcunché e dovrebbero cancellare o rendere anonimi i dati di traffico una volta che non siano più necessari alla comunicazione[154]. Il principio è, infatti, che i dati relativi alle trasmissioni elettroniche non debbano essere conservati oltre la finalità per i quali sono stati registrati in modo da garantire il ''diritto all'oblio''[155] dei movimenti di una persona nel *web*. Ciò per evitare che a distanza di tempo si possa ricostruire la navigazione in rete e, di conseguenza, le abitudini sociali dell'utente, assicurando una sorta di « diritto individuale alla disidentità »[156]. In questo caso non esiste alcun interesse costituzionalmente rilevante che possa giustificare il sacrificio del diritto alla riservatezza dell'utente telematico derivante dalla memorizzazione, dal trattamento e dalla conservazione dei dati di traffico oltre il tempo necessario per la connessione o la fatturazione in caso di servizi a pagamento. Una volta cessato il motivo tecnico (la trasmissione della comunicazione) o giuridico (la prova dell'avvenuta prestazione del servizio di comunicazione, *i.e.* la fatturazione) vengono meno le ragioni che hanno giustificato il « sacrificio dell'interessato » facendo riespandere nuovamente il diritto alla riservatezza come *right to be alone*[157].

Nel rispetto del diritto all'autodeterminazione individuale, *ex* art. 13 Cost.[158], per il quale è la persona a dover decidere in merito alla disponibilità delle proprie informazioni è previsto anche che, solo previo consenso dell'interessato, i dati menzionati possano anche essere raccolti ed utilizzati per fini diversi rispetto alla ricezione della comunicazione come ad esempio

---

cura di), *Il diritto della nuova economia: e-business, copyright, diritto dei consumatori*, Padova, 2002, 323.

[152] Si ricorda che questi ultimi soggetti sono anche quelli che, possedendo i dati anagrafici degli utenti ed assegnando i numeri identificativi dei computer connessi, sono in grado di individuare il titolare della linea chiamante.

[153] Ciò vale solitamente per i collegamenti ad Internet che avvengono attraverso la linea analogica.

[154] In tal senso V. CARIDI, *La tutela dei dati personali in Internet...*, cit., 775, 776.

[155] S. RODOTÀ, *Tecnopolitica: la democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997, 158 richiamato da V. GRIPPO-S. KIRSCHEN, *Dati relativi al traffico e alla fatturazione*, in M. ATELLI (a cura di), *Privacy e telecomunicazioni. Commentario al d.lgs. n. 171/1998*, Napoli, 1999, 84. Sul significato del diritto all'oblio T.E. AULETTA, *Diritto alla riservatezza e « droit à l'oubli »*, in G. ALPA-M. BESSONE-L. BONESCHI-G. CAIAZZA (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, 127 ss.

[156] G.E. VIGEVANI, *Comunicazioni dei dati di traffico per altre finalità*, in AA.VV., *Codice della privacy*, cit., 1681, che riprende il pensiero di C. DE GIACOMO, *Diritto, libertà e privacy nel mondo della comunicazione globale: il contributo della teoria generale del diritto allo studio della normativa sulla tutela dei dati personali*, Milano, 1999, 152.

[157] Così V. GRIPPO-S. KIRSCHEN, *Dati relativi al traffico e alla fatturazione*, cit. 85.

[158] Cfr. quanto considerato *supra* in par. 3.

per la fornitura di « servizi a valore aggiunto ». Un esempio può spiegare meglio la fattispecie. Attraverso un'analisi dei siti maggiormente visitati o dei messaggi pubblicitari aperti, è possibile individuare i gusti dell'utente e personalizzare la visita di un determinato sito *web* inserendo offerte promozionali più vicine ai suoi gusti. Questo tipo di servizio è 'aggiunto' rispetto alla semplice visualizzazione della pagina *web* richiesta perché utilizza i dati di traffico oltre quanto necessario per la trasmissione della comunicazione e la relativa fatturazione[159]. È indubbio che tale attività si traduca in un profitto per il titolare del trattamento che — solitamente finanziato dalle promozioni ospitate sul sito — trasforma l'ignaro utente in un potenziale cliente per le società di *marketing* che lo finanziano. Ecco perché le informazioni sul traffico hanno un valore economico e la persona, con le sue abitudini di navigazione, cessa di essere tale per divenire l'oggetto di una transazione[160]. Lungi dall'esprimere qualsiasi giudizio di valore sul funzionamento della cd. *net-economy*, in questa sede si vuole solo ribadire che il ''cittadino elettronico'' rimane l'unico titolare delle informazioni che riguardano la sua navigazione perché esse contribuiscono a formare la propria personalità ed identità individuale. In casi come questo è come se si cedesse una parte del proprio « corpo elettronico »[161], con la conseguenza che il singolo deve essere messo al corrente delle pratiche descritte e all'uopo poterle impedire non rinvenendo alcun interesse di maggiore valenza a fronte del quale dover limitare la tutela della persona. Le esigenze di *marketing* degli operatori di rete o il potenziale vantaggio economico da essi acquisito tramite il trattamento delle informazioni relative alla navigazione in rete rispondono ad interessi privati che non possono prevalere o essere bilanciati con valori di rango costituzionale di cui sicuramente il diritto alla riservatezza dell'utente telematico è espressione[162].

Da questo punto di vista, la scelta legislativa appare ragionevole, in quanto si autorizza l'attività esposta solo se l'utente — previamente informato delle modalità e della natura del trattamento *ex* art. 13 del d.lgs. 196/03 — presti il proprio consenso, revocabile in ogni momento, disponendo liberamente delle informazioni che gli appartengono.

Lo stesso principio è acquisito anche nella normativa comunitaria, recepito nel Codice della *privacy*, per cui gli Stati devono garantire la riservatezza delle comunicazioni elettroniche vietando l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o sorveglianza delle comunicazioni ad opera di persone diverse dagli utenti, salvo naturalmente la memorizzazione necessaria alla trasmissione della comunicazione o —

---

[159] Secondo la definizione della direttiva comunitaria, infatti, il servizio a valore aggiunto è « il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione » (direttiva 58/2002/CE, art. 2, lett. *g*), recepito con identico testo nel d.lgs. 196/03, art. 4, co. 2, lett. *l*). Alcuni esempi sono elencati nel considerando n. 18 della dir. 58/02 che ricomprende fra i servizi a valore aggiunto « consigli sui pacchetti tariffari meno costosi, orientamento stradale, informazioni sul traffico, previsioni meteorologiche, e informazioni turistiche ».

[160] S. Rodotà, *Proprietà*, Privacy *e Pornografia*, *le tre « P » di Internet*, cit., 240.

[161] S. Rodotà, *Proprietà*, Privacy *e Pornografia*, *le tre « P » di Internet*, cit., loc. cit.

[162] Sul fondamento costituzionale del diritto alla riservatezza cfr. *supra* par. 2.

considerando le informazioni personali come un bene disponibile — la prestazione del consenso da parte dell'utente[163].

8.1. *Il problema della conservazione per fini di sicurezza dei dati relativi alle comunicazioni trasmesse attraverso la rete Internet.*

Fermo restando quanto descritto, il problema della conservazione dei dati relativi al traffico telematico si scontra inevitabilmente con le nuove esigenze di sicurezza collettiva aventi origine soprattutto dalle cronache internazionali che hanno portato la Comunità europea ad intervenire recentemente in materia, cambiando in una certa misura il proprio punto di vista e limitando parzialmente quello che in precedenza è stato definito come il diritto all'oblio dell'utente Internet. Il nuovo intervento comunitario è stato ispirato dalla necessità di uniformare le discipline degli Stati membri in ordine alla conservazione dei dati di traffico telematico soprattutto per finalità di accertamento e repressione dei reati gravi nonché per implementare la lotta alla criminalità organizzata ed al terrorismo[164]. Da questo punto di vista è stato prescritto ''in via generale'' l'obbligo di conservare — per un periodo di tempo da sei mesi a due anni — i dati telematici necessari per rintracciare la fonte della comunicazione, la sua destinazione, la durata nonché le « attrezzature di comunicazione »[165].

La questione enunciata deve essere approfondita perché riapre il problema del rapporto fra *privacy* e sicurezza[166]. Le esigenze descritte dalla normativa di fonte europea rappresentano istanze e interessi di sicuro rilievo costituzionale. Non è dubbio che anche nel nostro ordinamento la salvaguardia dell'incolumità pubblica e la difesa dei cittadini — ostacolate dalla commissione di « reati gravi » ed annullate dall'operare di organizzazioni criminali e terroristiche — siano beni fondamentali — il cui valore è consacrato anche nell'art. 112 Cost. — che costituiscono il presupposto

[163] Direttiva 58/2002/CE, art. 5, co. 1.

[164] Cfr. *ibidem*, considerandi 9 e 21 nonché art. 1, paragrafo 1.

[165] Direttiva 54/2006/CE, art. 5. Lo Stato italiano non ha ancora recepito completamente la direttiva citata (il cui termine è fissato per il 15/9/2007) in quanto il relativo compito è stato, con la legge comunitaria 2006 (l. 6/2/07 n. 13, in G.U. 17/2/07 n. 40), delegato al Governo che dovrà intervenire entro 12 mesi dall'entrata in vigore della normativa.

[166] Invero, il problema enunciato si inserisce nell'ambito di un dibattito molto più ampio ed inerente, in generale, la relazione/dipendenza esistente fra libertà e sicurezza, nonché la possibilità ed i presupposti per limitare l'una in ragione della prevalenza dell'altra. Se è vero, infatti, che l'11 settembre 2001, l'emergenza terroristica, le recenti vicende politiche internazionali hanno « innalzato il bisogno collettivo di sicurezza », ciò non deve certo avvalorare « l'ipotesi di una pressoché assoluta dismissione delle garanzie connesse allo Stato costituzionale di diritto » (V. Baldini, *Tirannia della sicurezza nello stato costituzionale di diritto?*, in Id. (a cura di), *Sicurezza e stato di diritto: problematiche costituzionali*, Cassino, 2005, 8). Sulle medesime problematiche cfr. P. Ciarlo, *Sicurezza e Stato di diritto*, *ivi*, 19 ss.; G. De Vergottini, *La difficile convivenza fra libertà e sicurezza: la risposta delle democrazie al terrorismo. Gli ordinamenti nazionali*, Relazione tenuta al Convegno annuale dell'AIC, Bari, 17-18 ottobre 2003, in *www.associazionedeicostituzionalisti.it/materiali/convegni/aic200310/devergottini.html*.

per l'ordinario svolgimento e la partecipazione alla vita democratica del Paese, oltre che per il conseguente esercizio di tutte libertà costituzionalmente tutelate. In presenza di determinate condizioni e garanzie, tali interessi possono legittimamente limitare il diritto alla riservatezza dei singoli. Il costo di questo sacrificio[167] — in termini valoriali — dovrebbe però risultare economicamente vantaggioso. In altri termini dovrebbe trattarsi, tra le soluzioni possibili, di quella più efficace: di quella che tramite la limitazione o il sacrificio di un altro interesse costituzionale riuscisse a determinare un maggiore beneficio per la collettività rispetto alla sua difesa ad oltranza.

In tale contesto, quindi, non bisogna cadere nell'errore di trasformare la sicurezza in un mero ''richiamo di stile'' per violare irragionevolmente e senza condizioni la sfera personale dell'individuo. *Privacy* e sicurezza non sono due concetti che viaggiano necessariamente su binari separati potendo, al contrario, coesistere senza annullarsi reciprocamente[168].

La protezione delle comunicazioni elettroniche dalle interferenze altrui è un principio direttamente riconducibile anche all'art. 15 della nostra Carta costituzionale che garantisce la segretezza non solo della corrispondenza, ma di tutte le comunicazioni. La riservatezza della sfera personale dell'individuo, come si è già visto, è un valore costituzionalmente protetto che può affievolirsi solo quando sia compromesso un altro diritto anch'esso fondamentale. La questione è allora, da un lato, determinare quale siano gli altri termini di confronto in ragione dei quali possa accettarsi una limitazione della segretezza delle comunicazioni e, dall'altro, quale sia « un giusto punto di equilibrio »[169] nell'opera di bilanciamento degli interessi coinvolti.

La possibilità di conservare informazioni sugli utenti Internet rappresenta indubbiamente una compressione della sfera della riservatezza del singolo[170], e la Comunità europea individua specificamente una serie di interessi che possono giustificarne la pratica ovvero « la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica », « la prevenzione, ricerca, accertamento e perseguimento dei reati » nonché « l'uso non autorizzato del sistema di comunicazione elettronica »[171]. Si tratta evidentemente di esigenze che anche nel nostro ordinamento — come già detto — hanno una importanza fondamentale[172] e rispetto alle quali la stessa normativa comunitaria decide di affi-

---

[167] Discorre di « ''costo'' delle norme », come uno dei « test impiegati dalla Corte » costituzionale per giudicare della ragionevolezza della legge R. BIN, *Diritti e argomenti. Il bilanciamento degli interessi nella giurisprudenza costituzionale*, cit., 81 ss.

[168] Così G. BUTTARELLI, *Riservatezza ad alto rischio*, in *Il sole 24Ore*, 30 dicembre 2003, consultabile anche in *www.privacy.it/buttarelli06.html*. Sulla esistenza o meno di una relazione di tipo gerarchico fra libertà e sicurezza si interroga problematicamente E. DENNINGER, *Cinque tesi sull'architettura della sicurezza, in particolare dopo l'11 settembre 2001*, in V. BALDINI (a cura di), *Sicurezza e stato di diritto: problematiche costituzionali*, cit., 36 ss.

[169] L. CHIEFFI, *Centro elaborazione dati istituito presso il Ministero dell'Interno e tutela della riservatezza*, cit., 949.

[170] In relazione al forte condizionamento delle libertà fondamentali attuato attraverso la predisposizione di banche dati computerizzate A. BALDASSARRE, *Privacy e Costituzione*, cit., 423 ss.

[171] Direttiva 58/2002/CE, art. 15, co. 1.

[172] Sulla ricostruzione della tutela della sicurezza come valore fondamentale all'interno dell'assetto assiologico della nostra Costituzione V. BALDINI, *Sicurezza e li-*

dare ai legislatori nazionali, almeno parzialmente, il compito del rispettivo bilanciamento con la tutela della riservatezza dei singoli.

La direttiva citata rimanda alla discrezionalità degli stati membri in ordine alla scelta dell'*an* e del *quomodo* intervenire, prescrivendo che le relative misure debbano comunque essere « necessarie », « opportune » e « proporzionate » rispetto alle finalità indicate e consentendo, altresì, la possibilità di conservare i dati memorizzati per il periodo di tempo stabilito dalle leggi nazionali[173].

Con la nuova disciplina l'ordinamento comunitario[174] è intervenuto nuovamente in materia ritenendo necessario fissare comunque delle misure minime attraverso una serie di regole comuni, sopra descritte. Ciò senza escludere la possibilità che gli Stati membri possano in ogni modo, per le stesse finalità, prevedere anche regole ulteriori nel rispetto dei principi della direttiva citata.

8.2. *La sospensione delle disposizioni sulla cancellazione dei dati riguardanti il traffico delle comunicazioni elettroniche e la modifica dell'art. 132 del codice della* privacy.

Con l'art. 132 del d.lgs. 196/03 il legislatore italiano ha deciso di esercitare proprio la facoltà prevista dall'art. 15 della direttiva 58/2002/CE descritto, sebbene la valutazione politica del 'peso' da attribuire agli interessi della sicurezza e della tutela dei dati personali sia cambiata più volte in un breve lasso di tempo.

L'ultimo intervento nazionale in materia è stata la conversione in legge del decreto legge 144/05[175] che ha modificato profondamente il regime relativo alla registrazione dei dati riguardanti le comunicazioni elettroniche — per un verso — introducendo una disciplina transitoria operante fino al 31 dicembre 2007 e — per l'altro — modificando l'art. 132 del codice sulla *privacy* in merito all'obbligo di conservazione dei dati relativi alle comunicazioni elettroniche. Nello specifico, l'art. 6 del decreto legge citato ha sospeso fino al dicembre 2007 tutte le disposizioni normative inerenti la cancellazione dei dati riguardanti il traffico delle comunicazioni elettroniche sancendo l'obbligo, per i fornitori di accesso e di servizi internet, di conservare le « informazioni che consentono la tracciabilità degli accessi, nonché qualora disponibili, dei servizi » escludendo però espressamente la registrazione del 'contenuto' delle comunicazioni. Dopo la data indicata dovrebbero, invece, produrre effetti le modifiche all'art. 132 del codice sulla *privacy* che, in proposito, sancisce la possibilità di conser-

bertà nello stato di diritto in trasformazione, Torino, 2004, 66 ss.

[173] La Comunità europea lascia ai legislatori nazionali l'individuazione del ragionevole equilibrio fra la tutela della riservatezza nelle comunicazioni elettroniche e l'interesse alla sicurezza degli stati e alla repressione dei reati. Sul punto G.E. VIGEVANI, *Comunicazioni dei dati di traffico per altre finalità*, in AA.VV., *Codice della* privacy, cit., 1673.

[174] Direttiva 54/2006/CE.

[175] Decreto Legge 27 luglio 2005, n. 144, in G.U. 27 luglio, n. 173 (convertito, con modificazioni, in legge 31 luglio 2005, n. 155) intitolato « Misure urgenti per il contrasto del terrorismo internazionale ».

vare i dati relativi al traffico telematico per un massimo di dodici mesi complessivi, ma esclusivamente per finalità di accertamento e repressione di reati[176].

In tal modo, si è intervenuti incisivamente sulla precedente normativa contenuta nel d.lgs. 30 giugno 2003, n. 196 che consentiva la raccolta dei dati del traffico delle comunicazioni elettroniche ai soli fini della fatturazione o della contestazione del pagamento e per un periodo non superiore ai sei mesi. Inoltre, la memorizzazione per finalità diverse, come l'accertamento e la repressione dei reati, era consentita per i soli dati telefonici per una durata complessiva pari a quattro anni.

Il decreto legge in materia di terrorismo rappresenta l'ennesimo intervento governativo volto ad estendere il regime sulla registrazione dei dati riguardanti il traffico telefonico anche ad Internet sancendo l'obbligo generale della conservazione dei dati inerenti il traffico telematico, da parte dei fornitori di accesso e servizi internet, sino al 31 dicembre 2007. Stavolta, tuttavia, si sarebbe operato un passo indietro, almeno *prima facie*, rispetto ai precedenti interventi normativi escludendosi espressamente la raccolta dei dati inerenti il 'contenuto' delle comunicazioni telematiche ed elettroniche[177].

Non è dunque consentita, anche per il perseguimento della sicurezza pubblica, la conservazione, ad esempio, di messaggi di posta elettronica e dei relativi allegati, ma esclusivamente dei dati relativi alle coordinate cronologiche e temporali delle comunicazioni oltre a quelli del mittente e del destinatario.

Pur condividendo i principi ispiratori dell'intervento legislativo, se ne contestano i mezzi utilizzati che accomunando, anche solo parzialmente, la disciplina della conservazione dei dati telefonici con quelli telematici opera un bilanciamento non rigoroso perché confonde fenomeni fra loro diversi. Appare, infatti, una leggerezza postulare che la registrazione di dati di natura diversa e raccolti con mezzi tecnici differenti comporti una uguale compressione della riservatezza del singolo, pur se, in entrambi i casi, si esclude la conservazione del contenuto della conversazione e della comunicazione in generale.

---

[176] Precisamente per la durata di sei mesi « per finalità di accertamento e repressione dei reati » aumentati di altri sei mesi « per finalità di accertamento e repressione dei delitti di cui all'art. 407, co. 2, lettera *a*) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici e telematici » (art. 6, co. 3, d.l. 144/05).

[177] Già precedentemente, a pochi mesi dall'entrata in vigore del codice sulla *privacy*, fu, infatti, emanato il d.l. 354/2003 che, fra l'altro, prescriveva — per finalità di accertamento e repressione dei reati — la conservazione per la durata di cinque anni dei dati riguardanti non solo il traffico telefonico, ma tutte le altre comunicazioni compreso traffico internet e posta elettronica. In sede di conversione, tuttavia, il testo del decreto legge è stato modificato eliminando ogni riferimento alla conservazione dei dati riguardanti il traffico telematico proprio per le forti limitazioni che si sarebbero arrecate alla riservatezza del singolo. L'atto normativo *de quo*, infatti, si riferiva generalmente al traffico internet ed obbligava i fornitori di servizi a conservare per cinque anni anche tutti i dati relativi alla posta elettronica (mittente, destinatario, oggetto, contenuto, allegati); informazioni che — è facilmente intuibile — avrebbero consentito di ricostruire in maniera molto dettagliata abitudini e relazioni sociali o economiche di ognuno con chiara lesione dei principi costituzionali a tutela della vita privata della persona e della sua dignità.

Un conto, infatti, è la limitazione della *libertà informatica*[178], in certe condizioni e per un tempo determinato, causata dalla conservazione dei dati riguardanti il traffico telefonico che — limitandosi essenzialmente alla registrazione del numero chiamato, del giorno, dell'ora e della durata della conversazione — può essere solo parzialmente indicativa delle abitudini della persona e delle sue relazioni sociali. Un altro è la registrazione dei dati relativi al traffico telematico che può essere molto più invasiva della sfera della riservatezza della persona potendo, invece, rivelare una notevole quantità di informazioni anche sul 'contenuto' della comunicazione stessa.

Da questo punto di vista, l'art. 6 del d.l. 144/05 sancisce l'obbligo di conservazione di tutti i dati di traffico telematico che consentono la tracciabilità degli accessi e dei servizi. In pratica, ciò vuol dire effettuare non solo la conservazione delle informazioni relative all'utilizzo dei servizi, fra gli altri, di posta elettronica, *chat*, *newsgroup*, *ftp*, *filesharing*; ma anche dei dati relativi al giorno, ora, durata delle connessioni *web* nonché di tutti i numeri I.P. dei *servers* cui ci si connette — che nelle comunicazioni telefoniche equivarrebbe al numero di telefono chiamato — da cui è facilmente desumibile, ad esempio, l'indirizzo internet delle pagine consultate o almeno delle relative *homepage*. In tal modo, viene consentita la monitorazione degli accessi internet ed una definizione potenzialmente molto dettagliata dei gusti, delle abitudini e dell'identità sociale del singolo attraverso una semplice indagine sui siti maggiormente visitati, sulle pubblicità visualizzate o sulla tipologia dei gruppi di discussione cui si è partecipato. Sol che si pensi alla moltitudine di informazioni presenti sulla rete ed alle potenzialità della navigazione telematica, in teoria sarebbe possibile avere informazioni molto indicative anche su dati personali ritenuti sensibili e quindi meritevoli di una maggiore tutela[179]. Si immagini, per fare degli esempi, a chi naviga con una certa frequenza in siti di medicina riguardanti determinati tipi di malattie e faccia specifiche ricerche in materia, oppure al caso in cui si consultino costantemente le pagine relative a determinate confessioni religiose o a particolari gruppi di discussione. Si tratta, invero, di informazioni rappresentative di precisi interessi e potenzialmente rivelatrici anche dello stato di salute di una persona o dell'appartenenza ad una determinata comunità di fedeli, senza contare la facilità con cui in alcuni casi è possibile ricostruire anche le stesse inclinazioni sessuali del singolo.

Cade dunque in un equivoco chi ritiene che la registrazione dei soli dati di traffico Internet apporti un sacrificio del diritto alla riservatezza pari alla registrazione dei dati del traffico telefonico, dato che i primi sono parzialmente indicativi anche del contenuto della comunicazione elettronica.

Alla situazione descritta si aggiungono le prescrizioni del d.l. 144/05 che modificano l'art 132 del codice sulla *privacy* relative all'acquisizione dei dati di traffico, per finalità di accertamento e repressione dei reati san-

---

[178] Nell'accezione coniata da V. FROSINI, *Diritto alla riservatezza e calcolatori elettronici*, cit., 33, di potere di controllare le proprie informazioni personali ricadute nella disponibilità di terzi.

[179] Per i dati sensibili il codice della *privacy* prevede una disciplina diversa e più intensa. In particolare è previsto che per formazione delle relative banche dati sia necessario il consenso scritto dell'avente diritto nonché l'autorizzazione da parte del Garante dei dati personali (art. 26, d.lgs. 196/03).

cendo che gli stessi possano essere acquisiti entro sei mesi con un mero decreto motivato del pubblico ministero[180]. La mancanza dell'intermediazione del provvedimento di un giudice — espressamente abrogata dal decreto legge citato — si pone problematicamente al limite del rispetto della riserva di giurisdizione prevista dall'art. 15 Cost. per la quale le restrizioni alla libertà e alla segretezza di qualsiasi forma di comunicazione possono avvenire solo con atto dell'autorità giudiziaria[181].

Alla luce di queste considerazioni, l'art. 6 del d.l. 144/05 appare operare sacrificio della libertà del singolo non proporzionale rispetto al raggiungimento dei vantaggi che la normativa commentata appresterebbe, quali il raggiungimento di una maggiore sicurezza collettiva. E tale opinione, invero, non cambia neanche considerando che trattasi comunque di disposizioni dal carattere temporaneo che dovrebbero cessare i propri effetti a fine anno: il rischio è sempre quella di trasformare la *privacy* da diritto fondamentale ad « eccezione da dover essere giustificata »[182].

La discussione sulle questioni elencate deve essere pubblica e supportata da un'analisi degli « effetti a medio e lungo termine »[183] delle decisioni in materia di sicurezza e trattamento di dati personali le quali si ripercuotono non solo sulla tutela della riservatezza dell'individuo ma anche su tutti gli altri diritti e libertà fondamentali che inevitabilmente risultano coinvolti[184]. Allo stato attuale, la *privacy*, infatti, rappresenta una « nuova dimensione essenziale della libertà dei contemporanei », realizzando « la premessa per il pieno godimento della libertà di comunicazione, di manifestazione del pensiero, di associazione, di circolazione, della stessa libertà di impresa »[185].

Il ''costo assiologico'' derivante dal sacrificio del diritto alla riservatezza dei cittadini telematici sembra troppo alto rispetto all'interesse di prevenzione dei reati perché opera un sacrificio della libertà individuale della generalità dei consociati senza distinzione e per qualsiasi tipo di attività svolta. Per utilizzare un paragone — al di fuori della ''realtà virtuale'' — è come se per prevenire i reati fosse disposto che tutti i cittadini debbano essere pedinati e se ne debbano registrare gli spostamenti, con chi e quando si è aperta una corrispondenza, quando e che tipo di negozi o circoli si è visitato e così via.

La sorveglianza, al contrario, dovrebbe rimanere uno strumento di carattere eccezionale, limitato alle classi pericolose e non all'intera colletti-

---

[180] Sui problemi processual-penalistici sollevati dall'entrata in vigore del d.l. 144/05 R. CANTONE, *Le modifiche processuali introdotte con il « decreto antiterrorismo » (d.l. n. 144/05 conv. in l. n. 155/05)*, in *Cass. pen.*, 2005, 2507 ss.

[181] Dopo i sei mesi, invece, è comunque il giudice a dover autorizzare l'acquisizione dei dati, ma nei casi di urgenza il pubblico ministero può disporre l'acquisizione con decreto motivato che deve essere comunicato entro le successive quarantotto ore al giudice il quale deve convalidarlo entro le quarantotto ore successive. Va, in proposito, evidenziato come l'art. 15 Cost., al contrario dell'art. 13 e di riflesso dell'art 14, non prevede per le limitazioni della libertà di comunicazione l'intervento in via d'urgenza.

[182] L'espressione è di E. DENNINGER, *op. cit.*, 57.

[183] S. RODOTÀ, *L'occhio elettronico che sorveglia il mondo*, cit.

[184] *Relazione* dell'Autorità garante per i dati personale, anno 2003, cit.

[185] S. RODOTÀ, *La posta via Internet che è meglio cancellare*, in *La Repubblica*, 5 marzo 2004, p. 16. Sul punto anche A. BALDASSARRE, *Privacy e costituzione*, cit., 458 ss., 471; ID. *Globalizzazione contro democrazia*, cit., 257.

vità, evitando di trasformare « tutti i cittadini in potenziali sospetti »[186] attraverso un'indiscriminata ed illimitata formazione di archivi elettronici.

Oltretutto, la forte limitazione della sfera individuale più intima e riservata della persona, attuata attraverso la monitorazione delle comunicazioni elettroniche, è sfornita delle basilari garanzie costituzionali di cui all'art. 15 Cost. nel momento in cui è ammessa l'accessibilità ai relativi dati da parte di un semplice pubblico ministero e non attraverso l'autorizzazione di un giudice[187].

Infine, non vi è alcuna certezza sul fatto che la stessa sicurezza collettiva — che rappresenta il fine prefissato dal legislatore nazionale ed il valore che nel bilanciamento con l'interesse alla riservatezza del singolo è ritenuto prevalente — si realizzi efficacemente attraverso gli strumenti in precedenza descritti, i quali, paradossalmente, potrebbero avere proprio l'effetto inverso. Deve necessariamente essere considerato che, « in una società sempre più interessata, a fini pubblici e privati, ad accedere ed a utilizzare i più vari dati dell'individuo »[188], la formazione di banche dati così capienti e la conservazione delle informazioni per periodi così lunghi sconta paradossalmente l'effettiva difficoltà di garantirne una reale sicurezza e inviolabilità da parte di terzi non autorizzati[189] realizzando quello che è stato definito come « un pericoloso effetto boomerang »[190].

---

[186] S. Rodotà, *L'occhio elettronico che sorveglia il mondo*, in *La Repubblica*, 8 dicembre 2003; Id., *Discorso alle Camere* per la presentazione della Relazione dell'Autorità garante per la protezione dei dati personali, anno 2003, in *www.garanteprivacy.it*, p. 12. Sul punto anche E. Denninger, *op. cit*, 55 che fra le conseguenze dello stato di prevenzione ricorda la logica dell'agire orientato « non più soltanto secondo il pericolo (concreto, vicino) ma soprattutto secondo i rischi, non più secondo il sospetto dell'individuato ma secondo la potenziale e generale criminalità: nel rapporto fra cittadino e stato avrà luogo una generale inversione dell'onere di prova ».

[187] In questo caso non sembra neanche che possa farsi valere la distinzione fra dati esterni e dati interni della comunicazione, così come ricostruito dalla giurisprudenza di legittimità per i dati telefonici. I primi coinciderebbero con le informazioni contenute nei tabulati telefonici, mentre i secondi atterrebbero al contenuto della comunicazione. La natura del dato 'esterno' delle comunicazioni telematiche è diversa da quella delle comunicazioni telefoniche perché consente facilmente di ricostruire anche il contenuto della comunicazione stessa. È evidente, infatti, che dalla mera conoscenza dell'indirizzo della pagina *web* consultata si può risalire a buona parte del contenuto della comunicazione effettuata. Sulla distinzione fra dati esterni e dati interni delle comunicazioni telefoniche cfr. Cass Pen., Sez. un., 23/2/2000 n. 6, in *Cass. pen.*, 2000, 3595 con note di G. Melillo, *Intercettazioni ed acquisizioni di tabulati telefonici: un opportuno intervento correttivo delle Sezioni Unite*, *ivi*, 2602; L. Filippi, *Il revirement delle Sezioni Unite sul tabulato telefonico: un'occasione mancata per riconoscere una prova costituzionale*, *ivi*, 3246. Sul punto vd. anche Corte Cost. 17/7/1998 n. 281, in *Giur. it.*, 1999, 2006 con nota di A. Longo, *Il regime processuale dei dati esterni alla comunicazione: un problema ancora aperto*, *ivi*, 2006.

[188] G.E. Vigevani, *Comunicazioni dei dati di traffico per altre finalità*, cit., 1687.

[189] G.E. Vigevani, *op. cit. loc. cit.* Sul punto si rinvia anche agli esempi e alle considerazioni di A. Baldassarre, *Globalizzazione contro democrazia*, cit., 252 ss., che ricorda come persino i sistemi informatici che tradizionalmente sono considerati fra i più sicuri — come ad esempio quelli della Casa Bianca, della C.I.A. o dell'F.B.I. — non sono riusciti a sottrarsi dalla violazione dei cc.dd. *hackers* informatici.

[190] S. Rodotà, *L'occhio elettronico che sorveglia il mondo*, cit. Stesse perplessità in ordine alla affermazione che l'aumento della conservazione dei dati personali significhi effettivamente una maggiore sicurezza sono state espresse da F. Pizzetti, *Relazione annuale del Presidente dell'autorità Garante per i dati personali*, 2006, in *www.garanteprivacy.it*.

9. Altre tecniche di raccolta invisibile dei dati: *browsing chattering*, *cookies*, programmi *spyware*. Il ''diritto all'informazione'' del navigatore telematico.

Devono essere considerate separatamente, in ultimo, altre tecniche utilizzate dai fornitori di servizi internet per memorizzare informazioni sulla navigazione, sulle inclinazioni e sulle abitudini degli utenti telematici *indipendentemente da una loro collaborazione attiva*.

Nel *World Wide Web* l'utilizzo di ogni risorsa rappresenta la fruizione di un servizio come, ad esempio, la disponibilità di una casella di posta elettronica, la partecipazione a *forum* di discussione (*newsgroup* o *chat*), la ricerca di informazioni o anche solo la consultazione di una qualsiasi pagina Internet.

I fornitori di servizi *web* sono quindi la categoria più numerosa di operatori della rete ed anche quella più attenta alla registrazione ed alla creazione di profili degli utenti connessi.

Una prima serie di informazioni registrate da questi soggetti si realizza attraverso un'operazione chiamata *browsing chattering* al momento della digitazione dell'indirizzo della pagina *web* che si vuole visualizzare. Quando, infatti, si invia la relativa richiesta, il *server* che la riceve registra automaticamente, oltre il numero identificativo del computer connesso e l'indirizzo della pagina cercata, anche — a seconda del programma di navigazione — il tipo e la versione di *browser*[191] installato, i programmi che leggono i formati dei *files*, la lingua dell'utente[192]. Non si tratta, invero, di operazioni tutte funzionali alla trasmissione della comunicazione, con la conseguenza che la loro registrazione urterebbe contro il principio di necessità — stabilito dal codice sulla protezione dei dati personali — secondo il quale la raccolta delle informazioni inerenti l'individuo deve essere ''ridotta al minimo''[193]. La particolarità è che la registrazione di tali informazioni non dipende esclusivamente dalla volontà del titolare del trattamento, quanto dalle modalità di funzionamento tecnico della navigazione in Internet[194] e dalle caratteristiche dei programmi installati sul computer dell'utente per accedere alla rete. Ecco perché, in proposito, il Gruppo europeo per la protezione dei personali (art. 29, dir. 95/46) ha evidenziato come i *browsers* dovrebbero essere elaborati in modo da non trasmettere informazioni ulteriori rispetto a quelle necessarie per la trasmissione[195], spronando soprattutto le case fornitrici di *software* e *hardware* ad elaborare meccanismi che limitino i dati forniti[196].

---

191 Trattasi del programma utilizzato per la ricezione e la visualizzazione delle informazioni tramite Internet.

192 Per un'analisi dettagliata si rinvia al documento di lavoro 21 novembre 2000 del « Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali », cit., p. 16. Cfr. anche L.M. De Grazia, *Privacy e sicurezza nei contratti online*, in *Trattato breve di diritto della rete*, cit., 205-208.

193 D.lgs. 196/03, art. 3.

194 Sono conseguenze legate all'uso del protocollo di navigazione TCP/IP utilizzato in Internet.

195 Cfr. documento di lavoro 21 novembre 2000 del « Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali », cit., 100.

196 Raccomandazione 1/99 sul trattamento invisibile e automatico dei dati personali su Internet effettuato da *software* e *hardware*, adottata il 23/2/1999, 5093/98/IT/def., WP 17, in *www.garanteprivacy.it*.

Più complesso è il caso in cui oltre a tale tecnica vengano utilizzate anche altri strumenti per la raccolta invisibile dei dati come — tra gli altri — l'invio dei cc.dd. *cookies* o l'installazione di programmi *spyware*.

I *cookies*[197] sono dei piccoli *files* di testo inviati, durante la navigazione, da quasi tutti i server su cui risiedono le pagine *web* di cui si richiede la visualizzazione e che vengono poi memorizzati sulla memoria del computer dell'utente. Di solito, sono utilizzati per identificare inequivocabilmente il pc connesso[198] e possono contenere anche molte informazioni riguardanti il profilo dell'utente: username e password, frequenza e durata della connessione, *banners*[199] aperti, *link* di quel sito cui ci si è collegati consentendo una sorta di pedinamento virtuale[200].

Un software *spyware* è, invece un programma che, una volta installato sul computer, invia al fornitore informazioni riguardanti il sistema informatico e la navigazione in rete dell'utente[201]. La tipologia dei dati rivelati può essere più o meno invasiva — dalla registrazione della visita limitata ad alcuni siti alla memorizzazione di tutti i dati di traffico — a seconda della volontà del fornitore del programma e del tipo di dati che gli interessano. La particolarità risiede nel fatto che è difficile sapere di avere sul proprio computer un ''software spia'' perché si tratta in genere di applica-

[197] G. Ciacci, *La tutela dei dati personali su Internet*, in A. Loiodice-G. Santaniello (a cura di), *La Tutela della riservatezza*, cit., 376; V. Caridi, *La tutela dei dati personali in Internet. La questione dei logs e dei cookies alla luce delle dinamiche economiche dei dati personali*, cit., 779 ss.; E. Tosi, *Prime osservazioni sull'applicabilità della disciplina generale della tutela dei dati personali a Internet e al commercio elettronico*, in questa *Rivista*, 1999, 603; Id., *La tutela dei dati personali*, cit., 91.

[198] Un esempio banale può forse far capire meglio la funzionalità di tali strumenti. A volte accade che registrandosi ad un sito per visualizzare una sezione che richiede dei codici di accesso — ad esempio un servizio di posta elettronica — tutte le successive volte che ci si riconnette alla rete si apre, senza alcun inserimento di id e password, la pagina che dovrebbe essere personale: il sito *web* riconosce il PC ed il nome con cui l'utente si è registrato. A livello informatico ciò si spiega in quanto quasi ogni server al momento dell'apertura di una pagina *web* registra automaticamente sull'*hard disk* del navigatore un *cookie*, ossia un *software* che 'marca' il pc per identificarlo in rete e che, volendo, può inviare al sito che lo ha mandato una serie di informazioni riguardanti l'utente ogni volta che questi si riconnette a quella pagina *web*.

[199] Si tratta delle finestre pubblicitarie contenute nelle pagine *web*.

[200] Tendenzialmente i *cookie* sono leggibili solo dal fornitore del servizio che li ha inviati. Va ancora precisato, però, che non sempre i *cookie* sono inviati solo dal server che ospita la pagina richiesta ma spesso anche dai *banner* pubblicitari che compaiono al momento del collegamento. Tali messaggi promozionali, inoltre, il più delle volte non si trovano sul server cui corrisponde l'indirizzo digitato, ma su altri ai quali non si è chiesto il collegamento e che nonostante tutto si aprono automaticamente al momento della visualizzazione della pagina effettivamente richiesta. Ciò avviene attraverso l'utilizzo dei cosiddetti collegamenti ipertestuali invisibili (è quanto avviene comunemente, fra gli altri, nelle pagine *web* di Libero o Yahoo. Sul punto cfr. l'informativa sulla *policy privacy* contenuta nei relativi siti *web*: *www.yahoo.it*; *www.libero.it*).

[201] Tali programmi vengono anche chiamati « applicazioni E.T. » utilizzando un paragone con il noto film perché « dopo essersi insediati nel computer dell'utente ed avere appreso ciò che serve, essi fanno ciò che faceva l'extraterrestre di Steven Spielberg: chiamano casa » (documento di lavoro 21 novembre 2000, Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, cit., 50). Per un'analisi più approfondita V. Rossi, *Lo spyware e la privacy*, in G. Cassano (a cura di), *Diritto delle nuove tecnologie informatiche e dell'Internet*, Milanofiori-Assago, 2002, 184 ss.; L. Stilo, *Spyware: un ''parassita digitale'' dai mille ''untori''*, in *Nuovo diritto*, 2002, fasc. 9, 37 ss.

zioni legate all'utilizzo di altri programmi i quali, una volta installati, avviano anche lo *spyware* all'insaputa dell'utente. Questi strumenti sono solitamente nascosti in *software* gratuiti e le informazioni che riescono ad inviare rappresenterebbero, a detta dei fornitori, una sorta di controprestazione per il servizio prestato[202].

Tutti gli strumenti descritti — *browsing chattering*, *cookies*, programmi *spyware* — combinati o singolarmente possono creare un profilo molto dettagliato della persona connessa. Essi incidono sul modo con cui un soggetto viene presentato ''agli occhi del pubblico'' attraverso l'insieme delle informazioni che lo riguardano[203]. In questi casi sembra che vengano lesi proprio l'identità e la riservatezza della persona, né emergono, invero, altri interessi o beni costituzionalmente protetti con il cui bilanciamento potrebbe giustificarsi questo sacrificio.

L'utilizzo di queste tecniche è controverso ed anche le posizioni dottrinali sono molto diverse in merito alla loro regolamentazione.

Alcuni autori hanno, invero, tentato di diminuire la portata lesiva dell'utilizzo dei meccanismi di raccolta occulta dei dati perché non riuscirebbero a collegare le informazioni reperite con un effettivo titolare. In particolare, si è sostenuto che tutti i dati, eventualmente registrati dai fornitori di servizi Internet, sarebbero comunque anonimi in quanto associabili solo al numero che identifica il computer connesso (l'indirizzo IP) ma non anche ad un soggetto fisico determinato[204]. Infatti, l'unico operatore che potrebbe incrociare il numero che contraddistingue il computer con l'effettivo titolare della linea sarebbe il fornitore di accesso alla rete (l'*access provider*): i fornitori dei servizi *web*, quindi, potrebbero conoscere l'identità sociale di un individuo senza poterla ricollegare a quella anagrafica[205]. La tesi ripor-

---

[202] Le case produttrici di tali ''software di sorveglianza'' sostengono la liceità di tali strumenti in quanto le informazioni utilizzate non sarebbero direttamente riconducibili ad una persona fisica determinata ed oltretutto, non verrebbero comunque memorizzati dati sensibili (V. ROSSI, *Lo spyware e la privacy*, cit., 189). In realtà, deve essere ricordato che molto spesso l'utente, per utilizzare un programma, si registra fornendo i propri dati anagrafici e che la navigazione in rete può fornire molte informazioni su opinioni politiche, religiose o di salute (che sono dati sensibili). Negli USA, ultimamente, è stata sostenuta anche la tesi per cui l'utilizzo dello *spyware* sarebbe protetto dal primo emendamento. Sul punto criticamente N.W. PALMIERI, *USA: lo spyware protetto dalla libertà di espressione?*, in *www.interlex.it*, che ricostruisce, in proposito, la sorte della prima legge antispyware approvata negli USA. Si tratta dello *Spyware control act* approvata nello Stato dell'Utah e bloccato dal giudice federale che ha accolto la tesi della società *WhenU* — nota produttrice di software spia — in base alla quale la legge *antispyware* sarebbe stata contraria al principio costituzionale della libertà di espressione e della libertà del commercio interstatale (*Third judicial district Court*, *Salt Lake City*, 22/6/2004; per gli atti relativi all'intera vicenda *http://www.benedelman.org/spyware/whenu-utah/*).

[203] Così S. RODOTÀ, *Tecnologie e diritti*, cit., 109.

[204] In tal senso, soprattutto con riferimento all'utilizzo dei *cookies*, G. CIACCI, *La tutela dei dati personali su Internet*, cit., 380. L'A. sostiene che l'utilizzo dei *cookies* per ricercare informazioni sulla navigazione in rete non sarebbe invasivo della riservatezza della persona perché le navigazioni sarebbero anonime dato che il singolo sito registra solo l'IP del computer e non potrebbe risalire all'identità anagrafica dell'utente. In altre parole, i singoli siti *web* potrebbero sapere, ad esempio, che un utente collegatosi ad un computer contraddistinto con un certo numero *x* ha effettuato *tot* connessioni, per *tot* tempo, ha visitato *tot* link, e visto *tot* messaggi pubblicitari ma non potrebbero dire chi esso sia.

[205] Solitamente, per potersi collegare alla rete internet si stipula un abbonamen-

tata esclude che le informazioni prelevate con queste tecniche possano essere considerate come dati personali e che quindi non necessitino della medesima protezione giuridica.

Quanto descritto, tuttavia, è vero solo in linea di principio. Non esiste, infatti, una necessaria ''separazione delle funzioni'' fra operatori internet: chi fornisce l'accesso può fornire anche servizi. Di conseguenza, in questi casi attraverso l'utilizzo delle tecniche di raccolta occulta, di cui si è detto, è ben possibile tracciare un preciso *identikit* del navigatore telematico ricollegando i dati raccolti in maniera invisibile al titolare della linea connessa. Lo stesso risultato si ottiene nell'ipotesi, abbastanza frequente, in cui i gestori di siti *web* chiedono agli utenti di registrarsi con i propri dati anagrafici per poter usufruire di determinati servizi gratuitamente. Ecco perché un altro orientamento dottrinale ritiene che le informazioni prelevate durante la navigazione dai fornitori di servizi siano meritevoli di tutela giuridica solo se ricollegabili all'utente[206] con la conseguenza che in questo caso l'operatore telematico dovrà sottostare agli obblighi previsti per il trattamento dei dati personali.

Tuttavia, alla luce dei principi costituzionali a tutela della vita privata e delle definizioni contenute nella normativa nazionale e comunitaria, si ritiene di dover dissentire da entrambe le tesi riportate.

L'art. 4 del codice sulla *privacy*[207] definisce come dato personale « qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale ». La nozione è particolarmente ampia e ricomprende tutte quelle informazioni che possono essere *ricondotte alla persona* ''anche indirettamente'' come un numero di identificazione. Se le considerazioni svolte sono corrette, anche il numero che viene assegnato al computer per la connessione alla rete (*rectius* l'indirizzo IP)[208] e tutte quelle informazioni ad esso ricollegati[209] — dati di traffico, dati ottenuti

to — di norma, almeno per le connessioni di tipo analogico, gratuito — con un fornitore di accesso ad Internet (*Access Provider*). Questo, tutte le volte che si desidera navigare, attribuisce al computer richiedente un numero che serve ad identificarlo (il cd. numero IP). Quando l'utente digita, ad esempio, l'indirizzo della pagina *web* che vuole visualizzare, il *server* del fornitore del servizio su cui risiedono i dati registra il numero di identificazione del computer in modo da spedirgli le informazioni richieste. Il fornitore del servizio, quindi, dovrebbe conoscere solo il numero identificativo del pc del soggetto richiedente ma non anche la sua l'identità anagrafica, conosciuta solo dal fornitore di accesso ad Internet con cui si stipula il contratto di accesso.

[206] In tal senso V. Caridi, *La tutela dei dati personali in Internet*, cit., *passim*. Tale A. sostiene, ad esempio, che i dati registrati durante la navigazione (file di *log*) sarebbero dati personali solo se ricollegabili all'utente, ossia solo quelli del fornitore di accesso e non anche del fornitore di servizio, a meno che i due soggetti non coincidano (in part. p. 772). Analogamente, con riferimento alle informazioni carpite attraverso l'utilizzo dei *cookies*, ritiene che non si tratti di dati personali perché ricollegabili solo all'IP dell'utente e dunque non invasivi della sua riservatezza (p. 780). Sulla innocuità dei *cookie* se non riconducibili a soggetto preciso anche E. Tosi, *Prime osservazioni sull'applicabilità della disciplina generale della tutela dei dati personali a Internet e al commercio elettronico*, in questa *Rivista*, 1999, 604.

[207] Il testo — che non differisce dall'abrogato art. 1, co. 2, l. 675/46 — recepisce la definizione contenuta nell'art. 2 della direttiva 95/46/CE.

[208] G. Buttarelli, *Banche dati e tutela della riservatezza*, cit., 161.

[209] G. Arnò-A. Lensi Orlando, *op.*

attraverso il *browsing chattering*[210], dati ottenunti attraverso l'utilizzo dei *cookies* o di programmi *spyware* — sono dati personali. Infatti, queste informazioni si riferiscono sempre ad un persona identificabile attraverso il numero IP cui sono associate. Non si tratta allora di dati anonimi che chiunque può prelevare all'insaputa dell'utente, trattare come vuole e conservare per il periodo di tempo che desidera.

Il fatto che l'operatore non sia sempre a conoscenza dell'identità personale dell'utente cui si riferiscono non incide sulla meritevolezza della loro tutela. Le banche dati contenenti informazioni sulle abitudini degli utenti, infatti, hanno un importante valore economico per cui sono spesso rivendute a terzi e vengono anche messe all'asta quando una società fallisce. Oltretutto, può accadere che le società che gestiscono i servizi *web* vengano fuse o accorpate ad altre società operanti in rete. Le operazioni descritte facilitano la possibilità di unire dati di natura diversa con la conseguenza che un archivio elettronico in possesso di un fornitore di servizi che conteneva informazioni non collegate immediatamente ad una persona determinata può essere in seguito incrociato e confrontato con altre banche dati che potrebbero, al contrario, contenere i dati anagrafici dell'utente[211]. In proposito, si concorda con chi afferma che un dato sia « ''personale'' anche quando la sua concretezza informativa derivi da elementi integrativi in possesso di soggetti diversi dal titolare del trattamento »[212].

Ritenere che le informazioni relative alla navigazione, raccolte in modo occulto, non debbano avere alcuna protezione se non collegate immediatamente ad una persona determinata — eliminando forme di protezione

---

cit., 90 e citazioni nota 7. Tale dottrina sostiene che i dati raccolti in maniera occulta siano dati personali.

[210] Ritiene che i dati di traffico siano dati personali V. GRIPPO-S. KIRSCHEN, *Dati relativi al traffico e alla fatturazione*, in M. ATELLI (a cura di), Privacy *e telecomunicazioni. Commentario al d.lgs. n. 171/1998*, Napoli, 1999, 83, che a sostegno della propria tesi richiama il considerando n. 17 della direttiva 97/66/CE. Cfr., con particolare riferimento ai file di *log*, C. PARODI, *I file di log*, cit., 73.

[211] Le ipotesi descritte non sono affatto remote. Sul punto si rimanda agli esempi di vendite di dati e fusioni fra società descritti dal Gruppo per la tutela delle persone, nel lavoro 21/11/2000, *cit*. In merito, si vuole ricordare soprattutto l'esperienza della *DoubleClick*, una delle maggiori società pubblicitarie che opera su internet a livello internazionale elaborando profili degli utenti attraverso l'analisi del loro comportamento in rete. Il modo di agire di tale società è simile a tanti altri fornitori di servizi: « Doubleclick assegna un un numero di identificazione esclusivo ad ogni utente che visita uno dei siti *web* della rete DoubleClick e deposita un cookie, che verrà usato in seguito per identificare l'utente quando accederà ad un altro sito DoubleClick e, in base ai relativi dati, per personalizzare l'annuncio più adatto all'utente in questione. Anche se il visitatore non accetta il cookie, è comunque possibile elaborarne il profilo, in particolare se il suo indirizzo IP è di tipo statico » (p. 74). Nel 1999 la Doubleclick si è fusa con la società Abacus Direct che, facendo ricerche di mercato, aveva nelle proprie banche i nomi, gli indirizzi reali ed altre informazioni sulle abitudini di acquisto dei clienti (p. 50 e 75). La particolarità di Doubleclick, inoltre, è quello di collaborare con numerosissime altre società operanti in rete a livello mondiale (lo stesso portale 'Virgilio'), tanto che i *cookie* di tale società sono contenuti in quasi tutti i computer italiani collegati in rete.

[212] G. BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., 166, che precisa ancora: « per appurare l'idoneità di determinate informazioni a fini identificativi, appare sufficiente che si possa ipotizzare l'esistenza di altri dati ''personali'' che potrebbero essere intrecciati rendendo il soggetto identificabile, senza necessità di appurare il luogo ove sono custoditi e il relativo titolare » (*ivi*). Cfr. anche M. DALLA TORRE, in V. ITALIA-M. DALLA TORRE-G. PERULLI-A. ZUCCHETTI, Privacy *e accesso ai documenti amministrativi*, Milano, 1999, 241.

come l'informativa, il consenso, il divieto di cessione, l'accesso — significa aggirare il dettato normativo[213] e ledere la buona fede degli utenti. Questi ultimi verrebbero messi nelle condizioni di non sapere che le loro abitudini sono memorizzate oppure di credere che vengano registrate in maniera anonima; senza immaginare che incrociando opportunamente i dati con le informazioni in possesso di altri soggetti è possibile ricostruire tutti i loro movimenti con chiara lesione del diritto all'identità personale, perdendo la disponibilità di informazioni inerenti la propria personalità senza alcuna consapevolezza, né consenso, per fini non conosciuti e neanche espressione di interessi costituzionali che possano limitare legittimamente la *privacy* personale.

Anche il trattamento delle informazioni raccolte in forma invisibile deve rispettare le condizioni previste dalla legge per la protezione dei dati personali.

Le informazioni ottenute tramite il *browsing chattering*, ad esempio, dovrebbero essere considerate come dati relativi al traffico perché acquisite durante la trasmissione della comunicazione elettronica[214], con la conseguenza che, in mancanza del ''consenso informato'' *ex* art. 13 del codice, dovrebbero essere cancellati subito dopo la cessazione della trasmissione.

Più difficile è invece determinare la disciplina applicabile ai *cookies* ed ai programmi *spyware*. Tali tecniche a differenza delle altre, sono molto più invasive perché si realizzano attraverso una vera e propria intrusione nel sistema informatico dell'utente dal quale inviano informazioni. La memorizzazione di un *cookie* o l'automatica istallazione di un *software* di sorveglianza all'insaputa dell'utente rappresenterebbe una vera e propria violazione di quello spazio 'logico', ma privato, di pertinenza della persona che il legislatore ha tutelato come domicilio informatico[215].

La disciplina prevista dal codice per la protezione dei dati personali è abbastanza indicativa ma non esaustiva. L'art. 122 stabilisce, come principio generale, il divieto di accesso ad informazioni registrate nel terminale dell'utente e quello di memorizzazione o monitoraggio delle sue operazioni. Tuttavia, rimanda anche al codice di deontologia dei fornitori internet (art. 133) per la regolamentazione dei casi in cui è legittimo — previo consenso dell'abbonato sulla base di un informativa che indichi finalità e durata del trattamento[216] — derogare il divieto enunciato nel caso di « memo-

[213] Infatti, come bene viene messo in evidenza, per eludere « sistematicamente » le disposizioni sul trattamento dei dati personali basterebbe suddividere « gli elementi informativi di una banca dati in archivi separati collegabili all'occorrenza » e il gestore di un archivio potrebbe evitare gli adempimenti normativi « conservando informazioni apparentemente anonime e facendo custodire da terzi un determinato dato-chiave » (G. BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., 167).

[214] Cfr. definizione del codice sulla *privacy* e della direttiva 58/2002, art 2, nonché il considerando n. 15.

[215] Sul concetto si rimanda alle osservazioni contenute *supra* in par. 4. Ritengono che l'utilizzo dei *cookies* rappresenti una violazione domicilio informatico V. CARIDI, *La tutela dei dati personali in Internet*, cit., 783; S.F. BONETTI, *La tutela dei consumatori nei contratti gratuiti ad accesso ad Internet: i contratti dei consumatori e la privacy tra fattispecie giuridiche e modelli contrattuali italiani e statunitensi*, in questa *Rivista*, 2002, 1118; V. ROSSI, *Lo spyware e la privacy*, in G. CASSANO (a cura di), *Diritto delle nuove tecnologie informatiche e dell'Internet*, cit., 193.

[216] Tale informativa deve rispettare le indicazioni contenute nell'art. 13 del codice ed indicare: finalità e modalità del trattamento; natura facoltativa o obbligatoria

rizzazione tecnica necessaria alla trasmissione della comunicazione » o di fornitura di specifici servizi richiesti dagli utenti[217].

L'utilizzo di *cookies* e di *spyware*, quindi, non sarebbe del tutto illecito. In alcuni casi, indicati dal codice di autodisciplina, sarebbe possibile utilizzarli previo consenso del soggetto interessato. Va ricordato, in proposito, che non sempre l'utilizzo di alcuni di questi strumenti è dannoso. Alcuni *cookies*, ad esempio, sono utilizzati per facilitare e velocizzare il collegamento con la conseguenza che bisognerà operare le opportune distinzioni[218].

In attesta dell'autoregolamentazione degli operatori *web* si ritiene che, comunque, ogni sito dovrebbe, nel rispetto dell'interesse fondamentale alla vita privata dei singoli, informare chiaramente gli utenti circa l'esistenza di strumenti di raccolta invisibile delle informazioni e sulla natura e modalità del loro trattamento nonché rendere possibile il rifiuto dei marcatori o di altri simili dispositivi[219].

Ciò che, infatti, caratterizza Internet è l'assoluta mancanza di trasparenza nelle operazioni effettuate e nelle informazioni trattate; per cui le abitudini di ogni utente possono essere memorizzate e costantemente tenute sotto controllo senza alcun consenso del soggetto interessato. Quest'ultimo, oltretutto, dovrebbe essere considerato il soggetto debole del rapporto che intercorre con i fornitori di servizi internet che spesso subordinano la concessione di determinate applicazioni solo se i relativi strumenti di raccolta invisibile di dati (*cookie*, *spyware* ecc.) vengono accettati. Il navigatore spesso non immagina nemmeno che i dati che fornisce consapevolmente o inconsapevolmente costituiscono il più delle volte il prezzo per usufruire del servizio richiesto.

L'utente ha diritto a che le proprie informazioni non vengano prelevate senza la prestazione di un ''consenso informato'' su qualità e quantità dei dati trattati durante la navigazione. Il cittadino telematico è titolare delle informazioni che costituiscono il proprio patrimonio informatico e,

---

del conferimento dei dati; conseguenze di un eventuale rifiuto; soggetti terzi che possono prendere conoscenza dei dati; titolare del trattamento; nonché diritti che spettano all'abbonato/utente *ex* art. 7 (diritto di accesso, aggiornamento, rettifica, cancellazione ecc.).

[217] La disposizione recepisce l'art. 5 della direttiva 58/2002/CE.

[218] In proposito, deve essere precisato che, mentre lo *spyware* è invisibile e non si elimina disinstallando il programma che lo ha avviato, altri dispositivi come i *cookies* non sempre sono dannosi e possono essere facilmente individuati nel disco rigido di ogni computer ed eliminati. Oltretutto, gli ultimi programmi di navigazione consentono la possibilità di evitare l'invio dei *cookies*, di selezionarli o di essere avvisati quando sono inviati, in modo da poter scegliere quali accettare o meno. Per tale motivo, alcuni autori hanno dubitato della loro effettiva portata invasiva. Tuttavia, deve anche essere chiarito che è praticamente impossibile stabilire con certezza il contenuto di un *cookie* perché il *software* in esso contenuto è comunque scritto in un linguaggio accessibile solo a soggetti dalle specifiche competenze tecniche. Un comune utente non può stabile con esattezza, se non andandosene per una vaga idea, quali *cookie* cancellare o meno. Può capire il sito che li ha inviati e magari credere di essere garantito dal grado di affidabilità che ritiene di dare a quel gestore, ma pur potendone controllare il contenuto non può capire se effettivamente le informazioni che quel sito dice di trarre dal proprio computer corrispondono veramente a ciò che è scritto nel *cookie*.

[219] Sulle regole da apprestare cfr. anche i considerando n. 24 e n. 25 della direttiva 58/2002/CE e la Racc. 2/01, 17/5/01, relativa al requisiti minimi per la raccolta di dati *on-line* nell'Unione Europea, del Gruppo per la tutela delle persone fisiche con riguardo al trattamento dei dati personali (*www.garanteprivacy.it*).

dunque, di un vero e proprio *diritto all'informazione* su tutto ciò che riguarda la propria persona e che è rilevante ai fini della tutela della propria identità personale.

Tale diritto non è quello ''ad essere informati'' che solitamente si ricollega al diritto di cronaca e all'art. 21 Cost., ma è un diritto ad essere informati sulla *propria* persona e sulla disponibilità del proprio « corpo elettronico »[220] da parte di terzi. È un nuovo diritto strumentale, una precondizione, per la tutela della stessa libertà personale, intesa come rispetto della integrità della persona nella sua sfera intima e privata per preservarne la relativa dignità sociale (art. 3 Cost.).

Non si può accettare che il diritto alla riservatezza sia assicurato solo a chi abbia le conoscenze tecniche necessarie per potersi difendere dai pericoli della rete perché ciò si tradurrebbe in una vera e propria disparità di trattamento nei confronti dell'utente medio lasciato ''in balia'' delle regole della *net-economy* secondo le quali tutto è merce ed ogni 'click' su un pulsante di accesso è un indice di gradimento che viene riutilizzato a fini di *marketing* 'commercializzando' la persona. Sono gli stessi operatori della rete che di volta hanno un vero e proprio *dovere* di informare gli interessati sui rischi per la propria vita privata, sulle memorizzazioni effettuate relative alla navigazione, sulle modalità del trattamento e chiederne il consenso. Ciò, si ripete, anche se i dati prelevati non sono immediatamente ricollegabili ad una determinata persona perché esiste un interesse concreto ed attuale ad una *completa* informazione. Il singolo deve poter essere messo nelle condizioni di sapere che sta prestando un eventuale consenso al trattamento di dati ricollegati al proprio numero IP, ma che in futuro possono essere incrociati con altri archivi elettronici capaci di identificare i singoli anche anagraficamente[221].

10. Il problema dell'a-territorialità del fenomeno Internet e le conseguenze sulla tutela della riservatezza degli utenti. La necessità di avviare un dibattito di dimensione 'globale'.

Attraverso una panoramica generale delle questioni sollevate dall'evoluzione dei moderni strumenti di informazione è emersa l'affermazione di una nuova dimensione in cui il singolo sviluppa la personalità ed afferma la propria identità.

L'impiego delle tecnologie e la diffusione delle reti di comunicazione, infatti, sta progressivamente realizzando profondi cambiamenti nell'orga-

[220] L'espressione è di S. Rodotà, *Una scommessa impegnativa sul terreno dei diritti*, cit.

[221] Sono valide, in proposito, le indicazioni contenute nella Raccomandazione del Consiglio d'Europa del 23/2/99, che — da un lato — contengono un monito nei confronti degli utenti ricordandogli che l'uso di Internet non è comunque sicuro, che si lasciano sempre tracce elettroniche, che la migliore forme di tutela è l'anonimato; e — dall'altro — invita gli operatori *web* ad informare i navigatori sui rischi per la *privacy* ed a raccogliere i dati solo per fini espliciti e legittimi, a non comunicare a terzi i dati ricevuti, a non conservare i dati per un periodo superiore a quello necessario per realizzare le finalità del trattamento (Racc. n. R (99) 5 del Comitato dei ministri agli stati membri relativa alla protezione della *privacy* su Internet, 29/2/99 consultabile in *www.privacy.it*).

nizzazione pubblica, in quella imprenditoriale, così come nelle relazioni con i cittadini e nelle relazioni sociali[222]. La realtà cui si sta andando incontro è la creazione di « nuove comunità di interesse » sempre meno connotate geograficamente[223]. Come è stato evidenziato, « già oggi, molti professionisti trascorrono più tempo nel cyberspazio e si identificano più con il proprio indirizzo virtuale che con quello che definisce le loro coordinate geografiche »[224].

Il singolo acquista, allora, un'identità elettronica con un proprio indirizzo internet e la dottrina richiama la necessità di una tutela, oltre che del corpo fisico, di un « corpo elettronico ». Il legislatore, a sua volta, sembrerebbe aver preso cognizione dei cambiamenti descritti tutelando, ad esempio, il sistema informatico al pari del domicilio della persona, optando per una concezione ampia di « luogo di cui si disponga ''a titolo privato'' »[225] non legata alla materialità dell'ambiente eventualmente violato[226].

Dall'analisi svolta è, inoltre, emerso come la ''Rete delle reti'' sia un essenziale strumento per diffondere e raccogliere *informazioni*. Tuttavia, come si è cercato di mettere in evidenza, il concetto di 'informazione' in Internet è polivalente[227]. Essa non è solo il risultato, come si potrebbe essere portati a pensare, dell'esercizio della manifestazione del pensiero, del diritto di cronaca, di stampa, del diritto di informare ed essere informati. Il *world wide web* è anche un potente strumento di raccolta dell''informazione' che, talvolta, poco ha a che vedere con le libertà garantite dall'art. 21 Cost.

Tutti gli strumenti informatici, compreso Internet, sono quelli che più di ogni altro mezzo lasciano tracce e informazioni personali non sempre utilizzate in modo trasparente. Nella nuova società del consumo, passata da un sistema di produzione di massa ad uno di personalizzazione di massa[228], qualunque tipo di informazione diviene un bene economico oggetto di mercificazione[229].

---

[222] S. RODOTÀ, *L'occhio elettronico che sorveglia il mondo*, in *La Repubblica*, 8 dicembre 2003.

[223] J. RIFKIN, *L'era dell'accesso*, cit., 297, 298.

[224] J. RIFKIN, *op. cit. loc. cit.* D'altronde, anche in dottrina si sostiene come il riconoscimento della libertà informatica non è legato solo alle nuove tecniche di comunicazione informazione, ma debba coinvolgere anche la « libertà politica e l'organizzazione istituzionale » con riferimento ad esempio a quella che in prospettiva sarà la cd. democrazia elettronica con tanto di partecipazione e voto elettronico (T.E. FROSINI, *Tecnologie e libertà costituzionali*, in *Scritti in memoria di Livio Paladin*, cit., 849 ss.).

[225] A. PACE, *Problematica delle libertà costituzionali*, cit., 214.

[226] Sul concetto e sulle problematiche del domicilio informatico cfr. *supra* par. 4.

[227] D'altronde lo stesso termine 'informazione' è dotato di un'ampia poliedricità semantica. Cfr., per tutti, la dettagliata ricostruzione dei diversi significati attribuibili alla parola in esame effettuata a A. LOIODICE, *Contributo allo studio sulla libertà di informazione*, Napoli, 1967, 24-26 (nota 56).

[228] V. GRIPPO, *Analisi dei dati personali presenti su Internet. La legge n. 675/96 e le reti telematiche*, in *Riv. crit. dir. priv.*, 1997, 641, che riprende le parole di R. SAMARAJIVA, *Interactivity as though privacy mattered*, in P.E. AGRE-M. ROTENBERG (ed.), *Technology and privacy: the new landscape*, Cambridge, Massachussetts, 1997, 277. sul punto anche G. MACCABONI, *La profilazione dell'utente telematico fra tecniche pubblicitarie online e tutela della privacy*, in questa *Rivista*, 2001, 425; P. PALLARO, *La tutela della vita privata in relazione ai trattamenti di dati personali in Internet: l'approccio della Comunità europea*, in *Dir. com. sc. int.*, 2000, 7 ss., 12.

[229] Come è stato autorevolmente messo in evidenza, anche il dato più banale ha un valore economico perché non è la

Ne risulta che l'utente telematico viene coartato nell'esercizio del suo diritto all'"'autodeterminazione informatica''[230], ossia nella possibilità di decidere autonomamente quale debba essere il modo in cui conservare e trattare i dati riguardanti la propria persona, con la conseguenza di dover riconoscere a garanzia della sua sfera intima e personale — come si è visto — un nuovo ''diritto all'informazione'' sui rischi relativi alla propria vita privata che troverebbe il proprio fondamento costituzionale direttamente nell'art. 13 Cost.[231]

Le soluzioni trovate in materia dal legislatore nazionale e comunitario, da questo punto di vista, non sono ancora del tutto soddisfacenti anche perché rinviano, come nel caso della disciplina italiana, all'ulteriore fase regolativa dei codici di deontologia, peraltro ancora in corso di elaborazione.

Oltretutto, anche se è chiaro che i singoli ordinamenti non possono restare inerti di fronte all'evoluzione di Internet ed alle possibili lesioni dei diritti degli individui, non deve dimenticarsi che, poiché il fenomeno delle reti telematiche interconnesse ha una estensione globale, l'eventuale disciplina apprestata da un singolo governo può non ottenere il risultato sperato. Un'autonoma regolazione apprestata da un solo Stato risulta facilmente aggirabile attraverso la connessione e la trasmissione effettuata in un altro territorio dalla disciplina meno restrittiva. L'immagine ricorrente è quella di paesi che diventano « paradisi dei dati » — alla stregua dei paradisi fiscali — ai quali connettersi per non rispettare le regole stabilite da altri governi nazionali[232]. Il problema è concreto e fortemente incisivo sulla tutela della riservatezza dell'utente in rete, il quale deve tener conto che gli *standards* di protezione eventualmente apprestati dal proprio Stato non sono necessariamente rispettati anche dagli altri.

La disciplina del codice per la *privacy*, descritta nei precedenti paragrafi, si applica, infatti, unicamente a chi trasmette dall'Italia oppure a chi utilizza strumenti situati nel territorio nazionale salvo il caso in cui servano solo ai fini di transito[233]. Analogamente, i livelli di protezione previsti dalle direttive comunitarie sono effettivi solo per i paesi appartenenti all'Unione europea[234].

Di contro, Internet, per sua natura, non ha confini territoriali con la conseguenza che i dati possono essere prelevati, nella stessa CE, da un qualunque altro soggetto appartenente ad un paese terzo senza possibilità di estendere, ai confini di quest'ultimo, la relativa disciplina giuridica.

Ecco perché, uno dei principali problemi derivanti dall'affermazione di tale fenomeno globale, è la progressiva erosione del principio di sovra-

---

singola informazione ad avere importanza in sé e per sé, quanto « il contesto in cui viene inserita, [...] le finalità per cui viene adoperata, [...] le altre informazioni a cui viene collegata » (S. RODOTÀ, *Tecnologie e diritti*, cit., 83).

[230] M.G. LOSANO, *Il diritto pubblico dell'informatica*, cit., 16; E. DENNINGER, *Tutela ed attuazione del diritto nell'età tecnologica*, in *Nuovi diritti nella società tecnologica*, Atti del Convegno tenuto a Roma presso la LUISS, 5 e 6 maggio 1989, Milano, 1991, 65. Sul punto anche S. RODOTÀ, *Tecnologie e diritti*, cit., 106.

[231] Cfr. *supra* par. 9.

[232] S. RODOTÀ, *Tecnologie e diritti*, cit., 70.

[233] D.lgs. 286/03, art. 5.

[234] L'art. 4, direttiva 95/46/CE, prevede, infatti, il rispetto del principio dello 'stabilimento' per cui la normativa comunitaria si applica solo quando i titolari del trattamento abbiano la propria sede stabile in paese membro dell'Unione.

nità[235]. Gli stati non sono in grado di regolamentare autonomamente le relazioni che si svolgono nel proprio territorio, poiché chiunque può riuscire ad eludere facilmente le norme eventualmente apprestate. Quanto descritto è una diretta conseguenza della policentricità della struttura di Internet che permette di 'bypassare' l'eventuale blocco del flusso di dati attraverso la connessione ad un altro nodo della rete situato in qualsiasi parte del mondo. A livello tecnico sarebbe praticamente impossibile « impedire, o comunque gestire, la diffusione [di dati] verso solo alcuni Paesi collegati alla Rete e non altri »[236].

È anche per questo motivo che la normativa comunitaria, e di conseguenza quella nazionale, stabilisce il rispetto di particolari condizioni per il trasferimento dei dati al di fuori dell'Unione europea, vietandolo — salvo casi particolari[237] — quando « l'ordinamento del paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato »[238].

Il problema del flusso transfrontaliero dei dati è particolarmente controverso: basti pensare al fatto che — a causa del funzionamento tecnico della rete — le informazioni vengono trasmesse dividendole in pacchetti i quali possono prendere strade diverse e, almeno in teoria, passare per un paese estero piuttosto che un altro anche se la richiesta è effettuata ad un *server* della stessa nazione[239]. Il percorso dei dati non è predeterminato ed è « conoscibile solo *a posteriori* »[240].

La conseguenza è che in tutti questi casi si potrebbe realizzare un trasferimento di dati all'estero anche in paesi che non rispettano gli *standards* di protezione giuridica previsti dall'Unione.

Analogamente, pubblicare, ad esempio, in un pagina *web* dati e informazioni riguardanti altre persone potrebbe realizzare un flusso transnazio-

---

[235] In merito cfr. T. Ballarino, *Internet nel mondo della legge*, Padova, 1998, 33 ss. Sui problemi della deterritorializzazione, destatualizzazione e dematerializzazione del diritto ad opera dell'avvento delle tecnologie informatiche cfr. G. Pascuzzi, *Il diritto dell'era digitale*, Bologna 2002. Sul punto vd. anche J.S. Bauchner, *State sovereignty and the globalizing effects of the Internet: a case study of the privacy debate*, in *Brook. J. Int'l L.*, vol. 26, 2000-2001, 689, che evidenzia come « *The concept of sovereignty long has held center-stage in the field of international law. Nations define themselves by their territoriality and fight to protect their sovereign interests. Within this realm, the Internet has served as a unique globalizing force. In doing so, it has broken down traditional, physical boundaries, and, by extension, dismissed, or at least substantially modified, traditional view of state sovereignty* ». Cfr. anche R. Burnstein, *Conflict on the Net: Choice of Law in Transnazional Cyberspace*, in *Vand. J. Transnat'l L.*, 75, 1996, 82.

[236] G. Ciacci, *La tutela dei dati personali su Internet*, cit., 392-393.

[237] Sono quelli previsti dall'art. 43, d.lgs. 196/03 ossia, fra gli altri, l'esistenza del consenso espresso dell'interessato, l'esecuzione di obblighi derivanti da contratto, la salvaguardia di un interesse pubblico individuato con legge, la salvaguardia della vita e dell'incolumità fisica di un terzo, lo svolgimento di funzioni investigative. Cfr. anche l'art. 26 della direttiva 95/46/CE.

[238] D.lgs. 196/03, art. 45. che recepisce l'art. 25 della direttiva 95/46/CE.

[239] Tecnicamente la trasmissione dei dati avviene mediante la cd. ''commutazione di pacchetto'', una modalità attraverso la quale le singole informazioni vengono suddivise in una certa quantità di dati ed inviate singolarmente all'indirizzo di destinazione, con la particolarità che ogni 'pacchetto' può seguire un percorso diverso ed indipendente rispetto agli altri, per poi riordinarsi — attraverso la sequenza indicata su ognuno di essi — una volta arrivati a destinazione.

[240] V. Grippo, *Internet e dati personali*, cit., 308; Id., *Analisi dei dati personali presenti su Internet. La legge n. 675/96 e le reti telematiche*, cit., 665 ss.

nale di dati poiché il sito è visibile contemporaneamente in ogni parte del mondo[241].

La questione è interpretativa. Occorre capire se il *trasferimento* di cui parla la direttiva comunitaria possa ritenersi comprensivo sia del ''passaggio materiale'' di dati da un soggetto ad un altro, sia della loro ''mera visualizzazione'' in un paese non facente parte dell'UE. Se si accettasse questa seconda ipotesi, si arriverebbe alla conseguenza paradossale che tutte le volte in cui si immettono dati su un sito *web* si realizzerebbe un flusso transnazionale di dati che viola costantemente la normativa comunitaria dato che non è possibile limitare la visione di una pagina internet ai soli paesi che osservano le regole di fonte europea.

Sul punto è intervenuta anche la Corte di giustizia CE, chiarendo diversi aspetti della disciplina sul trasferimento dei dati. In particolare, con una sentenza del novembre 2003[242], i giudici di Lussemburgo hanno stabilito alcuni principi chiave. Il giudizio aveva ad oggetto proprio la pubblicazione, da parte di una cittadina svedese, di una pagina *web* in cui erano state inserite informazioni sulle mansioni dei colleghi o sulle loro abitudini nel tempo libero, con l'indicazione, in alcuni casi, anche di nomi, cognomi, situazioni familiari o recapiti telefonici. Il rinvio pregiudiziale alla Corte era stato sollevato per la contestata interpretazione di alcune disposizioni della direttiva 95/46 in merito al trattamento dei dati personali delle persone fisiche.

Fra le norme violate ci sarebbero state, infatti, quelle sul flusso transfrontaliero dei dati personali poiché, a detta del ricorrente, l'immissione di informazioni in una pagina Internet — che per sua natura è visibile in qualsiasi parte del mondo — avrebbe realizzato un trasferimento di dati anche in paesi che non assicurano un livello adeguato di tutela del trattamento dei dati personali violando l'art. 25 della direttiva comunitaria 95/46.

La Corte, tuttavia, non ha accolto la tesi avanzata considerando che la disposizione non definisce cosa debba essere inteso per trasferimento e che la direttiva 95/46 è stata elaborata senza tener conto del fenomeno Internet. Secondo i giudici comunitari — anche in base alle intenzioni del legislatore — la pubblicazione sul *web* effettuata dalla cittadina svedese non poteva essere considerata alla stregua di un trasferimento di dati verso un paese terzo solo perché visualizzabile anche all'estero.

Un diverso ragionamento, si è detto, avrebbe comportato l'applicazione generale della disciplina speciale per il trasferimento dei dati nei paesi extraeuropei per tutte le informazioni immesse in rete. La conseguenza sarebbe stata la creazione di un, improbabile e inattuabile, obbligo in capo

---

241 A. Oliva, *La tutela penale del diritto alla privacy in Internet*, cit., 92; G. Ciacci, *Internet e diritto alla riservatezza*, in *Riv. trim. dir. e proc. civ.*, 1999, 248.

242 CGCE, 6 novembre 2003, causa C-101/01, in questa *Rivista*, 2003, 1079 ss. A commento della sentenza cfr. le note di A. Palmieri-R. Pardolesi, *Il codice in materia di protezione dei dati personali e l'intangibilità della « privacy » comunitaria*, in *Foro it.*, 2004, IV, 59; R. Panetta *Trasferimento all'estero di dati personali e Internet: storia breve di una difficile coabitazione*, in *Europa e dir. priv.* 2004, 1002; G. Cassano-I.P. Cimino, *Qui, là, in nessun luogo... Come le frontiere dell'Europa sia aprirono ad Internet: cronistoria di una crisi annunciata per le regole fondate sul principio di territorialità*, in *Giur. it.*, 2004, 1805.

agli Stati membri di « impedire qualsiasi immissione in Internet di dati personali »[243].

Il caso esaminato ha risolto alcuni legittimi dubbi emersi già nel dibattito dottrinale, ma dimostra ulteriormente come l'interpretazione letterale delle norme vigenti, elaborate senza tener conto dell'avvento delle nuove tecnologie informatiche, possa portare a risultati sproporzionati rispetto alle finalità per le quali erano state approvate.

È, allora, sicuramente necessario rielaborare le categorie tradizionali (sovranità, domicilio, diritto all'informazione *etc.*), in ragione delle nuove esigenze legate al continuo sviluppo di Internet. Tuttavia, il dibattito non può essere limitato alla singola nazione ma deve necessariamente coinvolgere l'intera comunità connessa alla rete. Già lo sforzo di apprestare in determinati settori una disciplina uniforme a livello europeo rappresenta evidentemente un passo avanti. Ciononostante — come si è cercato di evidenziare — il mancato coinvolgimento anche di pochi paesi può rendere vano qualunque sforzo regolativo. Una eventuale disciplina che voglia essere davvero effettiva dovrebbe essere, più che sovra o inter-nazionale, realmente globale.

[243] CGCE, 6 novembre 2003, cit., punto 69 della decisione.