CLIZIA D'AGATA

« *SELF* » E « *STRICT* » *REGULATION*: IL TRATTAMENTO VIA *INTERNET* DEI DATI PERSONALI NELL'APPROCCIO « PLURIDISCIPLINARE » DI TUTELA INTRODOTTO DAL CODICE DELLA *PRIVACY*

1. Introduzione.

Lo sviluppo degli strumenti telematici e la diffusione di *Internet* hanno creato, negli ultimi anni, uno « spazio virtuale » in cui milioni di individui riescono simultaneamente a trasmettere e ricevere informazioni[1]. La Rete rende accessibile la comunicazione tra *computers* lontani chilometri, consente agli utenti di dare larga diffusione alle loro idee e permette loro di concludere operazioni economiche[2].

Queste caratteristiche hanno determinato il sorgere di nuove e pericolose forme di invasione della *privacy* degli individui[3], trasformando ogni collegamento dell'utente alla Rete in una fonte inesauribile di informazioni

[1] Cfr. G. Cassano, *Commercio elettronico e tutela del consumatore*, Giuffrè Ed., Milano, 2003; G. Corasaniti, *Esperienza giuridica e sicurezza informatica*, Giuffrè Ed., Milano, 2003; C. Rossello, G. Finocchiaro e E. Tosi (a cura di), *Commercio elettronico, documento informatico e firma digitale:la nuova disciplina*, Giappichelli Ed., Torino, 2003; G. Ziccardi, *Crittografia e diritto: crittografia, utilizzo e disciplina giuridica, documento informatico e firma digitale, segretezza dell'informazione e sorveglianza globale*, Giappichelli Ed., Torino, 2003.

[2] Il mondo della comunicazione telematica fa ormai parte dell'ambiente lavorativo e, spesso, familiare dell'individuo. *Internet* è esso stesso spazio in cui il cittadino conduce una propria « vita telematica », attraverso la partecipazione a *forum* di discussione, *chat rooms* o mediante la conclusione di contratti *on-line*. In tal senso cfr. Sciumè, *Riflessi giuridici della comunicazione telematica: Internet, offerta di prodotti e servizi e tutela della privacy*, in C. Vaccà (a cura di), *Il commercio elettronico: il documento digitale, Internet, la pubblicità on-line*, Milano. Egea, 1999, 148.

[3] Cfr. R. Pardolesi, *Dalla riservatezza alla protezione dei dati: una storia di evoluzione e discontinuità*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè Ed., Milano, 2003, 20 ss.

personali. I dati vengono associati l'uno all'altro per la formazione di profili personalizzati, attraverso una pratica che trasforma di fatto la sfera privata dei cittadini in privilegiata merce di scambio commerciale[4]. La società telematica, del resto, ha sviluppato un mercato in cui i beni acquistano valore in base al loro grado di connessione con i bisogni immateriali della persona[5]: l'utilizzo dei dati avviene per fini economici e l'intera esistenza dell'individuo risulta oggetto di operazioni commerciali al pari delle altre merci[6].

La situazione appena descritta pone all'attenzione del giurista la necessità di ricorrere a nuove tecniche di regolamentazione della *privacy* in *Internet*, in grado di fornire un'adeguata protezione agli utenti sia in termini di sicurezza, sia in termini di riservatezza[7]. Tale operazione richiede un'analisi critica delle attuali politiche di tutela dei dati personali in Rete, attraverso una disamina delle differenze esistenti tra l'approccio di *Strict-Regulation*[8], adottato dalla Comunità Europea, e quello di *Self-Regulation*[9], proprio del sistema giuridico statunitense[10].

---

[4] Le strategie di *marketing* hanno esteso la loro portata proprio in riferimento al trattamento dei dati personali via *Internet*. La Rete offre alle imprese non solo la possibilità di sponsorizzare i propri prodotti in maniera veloce ed efficace, attraverso l'invio di *e-mail*s pubblicitarie, ma anche di aggregare le informazioni degli utenti ai fini di una « profilazione » dei consumatori indispensabile nell'attuale sistema di produzione e distribuzione delle merci. In proposito si è parlato di sistema di « personalizzazione di massa ». Cfr. G. Maccaboni, *La profilazione dell'utente telematico fra tecniche pubblicitarie on-line e tutela della privacy*, in questa *Rivista*, 2001, 425.

[5] Cfr. Rifkin J., *L'era dell'accesso*, Milano, Mondatori, 2000, 34 ss.; cfr. Castells M., *The information age*, Oxford, Blackwell, 1998, 67.

[6] Cfr. Simitis S., *Il contesto giuridico e politico della tutela della privacy*, in *Riv. Crit. Dir. priv.*, 1997, 574.

[7] Cfr. F. Di Ciommo, *Evoluzione tecnologica e regole di responsabilità civile*, Edizioni Scientifiche Italiane, Napoli, 2003, 20 ss.

[8] Per *Strict-Regulation* si vuole intendere l'approccio con il quale le Istituzioni adottano strumenti normativi (leggi, direttive, regolamenti ecc.), a tutela dei diritti di *privacy* dei cittadini. Tale sistema trova applicazione in riferimento alle politiche di tutela dei dati personali adottate dalla Comunità Europea ed è caratterizzato dall'adozione del principio di *opt-in* e dal ruolo di garanzia, controllo e vigilanza svolto dalle Autorità Indipendenti. Espressione di tale approccio è la Direttiva 95/46/CE che introduce un sistema fondato sul diritto all'autodeterminazione informativa dell'individuo, sulla trasparenza nelle attività di trattamento e sui diritti di accesso, rettifica, cancellazione dei dati. In modo particolare, l'attenzione viene rivolta all'istituto del consenso (come manifestazione di volontà libera, specifica ed informata), nell'ambito di una concezione della *privacy* quale diritto al controllo « procedimentalizzato » delle proprie informazioni. Una definizione di « *European tradition of Strict Protection of the individual's right to privacy* » è stata data da *Lyombe Eko, Many spiders, one worldwide web: towards a typology of Internet Regulation, 6 Comm. L. & Pol'y 445* (2001). Altrimenti si è anche parlato di « *Law-Regulation* », cfr. D. Calenda, *Il dibattito internazionale sui limiti e le tendenze delle politiche per la tutela della privacy in Internet*, in *Riv. It. Dir. Pub. Com.*, 2000, I, 531 ss.; oppure di « *Government-Regulation* », cfr. P.G. Smith, *Free Speech on the World Wide Web: a comparison between French and United States policy with a focus on UEJF v. Yahoo! Inc.*, *21 Penn St. Int'l L. Rev.* 319 (2003).

[9] Al suo interno manca ogni riferimento ad una normativa di carattere generale, la cui adozione trova avversari irriducibili nei principi del libero mercato e della non interferenza dello Stato nei rapporti tra privati. Il risultato è quello di un sistema di protezione delle informazioni in cui la tutela viene delegata agli stessi « attori » del mercato (*Internet Service Providers* ed utenti), attraverso pratiche di autoregolamentazione e strumenti di *self-help*.

[10] In questa sede, si fa esclusivo riferimento al trattamento operato nella Rete da soggetti privati. Non si deve trascurare in-

Il primo, ha mostrato evidenti limiti in ordine all'applicazione del principio del consenso preventivo dell'interessato. Il quadro di forte asimmetria informativa e le profonde disparità di potere negoziale presenti nella Rete[11], hanno evidenziato il pericolo che il consenso fosse solo teorico, ovvero che, in mancanza dello stesso, l'interessato fosse impossibilitato ad avvalersi di determinati servizi o prestazioni[12]. Il meccanismo del consenso, inoltre, si è posto in netta contrapposizione con le caratteristiche di velocità, rapidità ed immediatezza della comunicazione elettronica: una sua applicazione rispettosa, infatti, rischia di tradursi in una richiesta continua ed incessante dello stesso, con il consequenziale rallentamento dei tempi di comunicazione e l'aumento dei costi di collegamento a carico degli utenti[13].

Il sistema di *Self-Regulation*, a sua volta, ha posto problemi in merito alla mancanza di un apparato di controllo in grado di vigilare sul rispetto delle norme create autonomamente dagli operatori del settore. Questo ha provocato incertezze sia in ordine al contenuto delle regole, eccessivamente legate agli interessi personali di cui sono espressione, sia in rapporto alla loro effettiva applicazione[14].

I limiti di entrambe queste politiche di protezione, rendono evidente la necessità di configurare un nuovo approccio di tutela della *privacy* in Rete, capace di porsi quale alternativa a quelli appena descritti. Caratteristica principale della nuova disciplina dovrebbe essere il contemporaneo intervento di leggi e norme di autoregolamentazione, attraverso la determinazione di un sistema in cui alla fonte legislativa vengano affiancate fonti normative ulteriori[15].

---

fatti, la presenza nel sistema nord americano, di precise e puntuali regole di carattere federale relative all'elaborazione di dati effettuata dai poteri pubblici. È sufficiente ricordare il tenore del *Privacy Act* del 1974 per ritrovare anche negli Stati Uniti una regolamentazione fondata sul consenso e sulla trasparenza delle informazioni rese all'interessato.

[11] Cfr. G. Comandè, *Commento agli artt. 11-12*, in E. Giannantonio, M.G. Losano, V. Zeno-Zencovich (a cura di), *La tutela dei dati personali. Commentario alla l. 675/96*, Padova, Cedam, 1999, 149.

[12] La cessione dei dati è divenuta, nella maggior parte dei casi, condizione indispensabile alla fruizione di beni e servizi, rendendo l'individuo « prigioniero » delle proprie informazioni e privo di ogni potere di decisione in merito al flusso dei dati che lo riguardano. Cfr. P. Morozzo della Rocca, *Commento all'art. 12*, in C.M. Bianca, F.D. Busnelli (a cura di), *Tutela della privacy, Commentario*, in *Nuove leggi civ.*, 1999, 367; G. Buttarelli, *Banche dati e tutela della riservatezza*, Milano, Giuffrè editore, 1997, 284. In quest'ottica, S. Rodotà ha riconosciuto nella *privacy* non soltanto il potere di mantenere il silenzio su se stessi, quanto l'espressione della libertà delle scelte esistenziali, nell'ottica di « un integrale recupero della sovranità su di sé, che faccia della pienezza della sfera privata anche la condizione della pienezza della sfera pubblica ». Cfr. Rodotà S., *Prime note sistematiche sulla protezione dei dati personali*, in *Riv. Crit. Dir. priv.*, 1997, 590 ss.

[13] Tutto questo avrebbe il risultato di distogliere l'attenzione degli utenti dallo strumento del consenso, che verrebbe ceduto al solo fine di procedere senza intralci nella navigazione.

[14] Tutto questo si è tradotto, negli Stati Uniti, nell'accettazione di pratiche invasive della *privacy* degli utenti, come l'invio di comunicazioni non sollecitate, l'utilizzazione dei *cookies*, la conservazione dei *logs* da parte dei *providers*, considerate, dalla letteratura giuridica statunitense, pienamente legittime. Cfr. F. Di Ciommo, *Diritti della personalità tra media tradizionali e avvento di Internet*, in G. Comandé (a cura di), *Persona e tutele giuridiche*, Giappichelli Ed., Torino, 2003, 44 ss.

[15] In questo senso si è parlato di « *co-regulation* », ovvero di un processo regolatore che « affidi l'intera materia ad un policentrismo di fonti, collocate in una coordinata sequenza a vari livelli: una cornice

Da una parte, infatti, si manifesta l'esigenza di una normativa di rango legislativo, capace di regolamentare in via generale i fenomeni che nella Rete possono dar adito ad illegittime intrusioni nella sfera personale degli utenti.

Dall'altra, è necessario un intervento che si spinga più nello specifico[16] e che, attraverso le regole prodotte dagli stessi operatori del settore interessato, sia in grado di interpretare le nuove esigenze della comunicazione telematica.

Un ruolo di non poca importanza deve, inoltre, essere attribuito agli strumenti tecnologici di carattere informatico[17] ed all'attività di controllo di un'autorità amministrativa indipendente[18]. I primi, hanno il pregio di produrre un supporto tecnico in grado di dare attuazione concreta alle previsioni normative[19].

La seconda, assume un ruolo di fondamentale importanza in qualità di organo « autonomo »[20], mostrandosi in grado di riequilibrare le disuguaglianze informative esistenti tra i soggetti coinvolti dall'attività di circolazione dei dati.

Il sistema di tutela così concepito si pone a cavallo tra le politiche di « *Strict* » e di « *Self* » *Regulation* fino ad ora adottate, delineando un approccio « pluridisciplinare » di protezione, in grado di adeguarsi ai caratteri di un'evoluzione tecnologica che si presenta incessante ed impetuosa. Queste caratteristiche pongono le premesse per la configurazione di una « nuova » forma di regolamentazione della *privacy* in Rete, la cui applicazione sarebbe in grado di accordarsi sia ai caratteri dell'ordinamento statunitense sia alle tradizioni giuridiche europee.

---

legislativa, la specificazione delle regole mediante leggi nazionali, l'adozione di codici modello di formazione autodisciplinare ». Cfr. S. ZIRONI, *Privacy e reti telematiche*, in *Il dir. d'aut.*, 2003, 428.

[16] Cfr. G. PINO, *I codici di deontologia nella normativa sul trattamento dei dati personali*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, cit., 760 ss.

[17] Sull'argomento cfr. F. BERGHELLA, *La sicurezza dei dati e dei sistemi*, in R. ACCIAI (a cura di), *Il diritto alla protezione dei dati personali: la disciplina della privacy alla luce del nuovo Codice*, Maggioli S.p.A., Santarcangelo di Romagna, 2004, 229 ss.

[18] Cfr. G. BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., 489 ss.

[19] Lo sviluppo dell'industria informatica deve essere volto alla realizzazione di tecnologie il più possibile « neutre », le cui applicazioni rispettino le disposizioni normative a tutela della sfera privata, adeguandosi ai principi di proporzionalità e di necessità nella raccolta e nel trattamento dei dati personali. Cfr. S. MELCHIONNA, *I principi generali*, in R. ACCIAI (a cura di), *Il diritto alla protezione dei dati personali: la disciplina della privacy alla luce del nuovo Codice*, cit., 29 ss. In tal senso si è espresso più volte il Gruppo dei Garanti Europei, incoraggiando l'industria del *software* e dell'*hardware* a creare prodotti *Internet* rispettosi dei principi di tutela della riservatezza. Tra i documenti più recenti cfr. il « *Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group* », adottato il 23.01.2004, WP 86 (MARKT/11816/03/EN) reperibile sul sito www.*europa.eu.int/comm/internal_market/privacy/workingroup_en.htm*

[20] Sulla natura giudica del Garante per la protezione dei dati personali cfr. A. LIROSI, *Il garante per la protezione dei dati personali*, in V. CUFFARO e V. RICCIUTO (a cura di), *Il trattamento dei dati personali. Vol. II: profili applicativi*, Torino, Giappichelli, 1999, 398 ss. Per un più ampio commento in ordine alla caratteristiche del Garante, vedi inoltre: C. LACAVA, *Commento all'art. 30*, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *Tutela della privacy*, *Commentario*, cit., 695 ss.; R. D'ORAZIO, *Commento all'art. 30*, in E. GIANNANTONIO, M.G. LOSANO, V. ZENO-ZENCOVICH (a cura di), *La tutela dei dati personali. Commentario alla l. 675/96*, cit., 292 ss.

Le pagine che seguono si propongono di chiarire tale affermazione, attraverso un'analisi delle caratteristiche che contraddistinguono il nuovo approccio di tutela e le sue modalità di applicazione. A tal fine, l'attenzione sarà rivolta alle forme di *Self-Regulation* adottate negli Stati Uniti, con lo scopo di presentare l'approccio « pluridisciplinare » quale auspicabile alternativa. Parimenti, l'analisi sarà rivolta alla disciplina europea, esemplificata dal Codice della *Privacy* recentemente emanato in Italia, quale modello per l'attuazione del sistema « pluridisciplinare » appena descritto.

2. Dalla crisi della Self-Regulation all'esigenza di un approccio « pluridisciplinare » di tutela: l'esempio degli Stati Uniti.

I vantaggi dell'approccio « pluridisciplinare » risultano con chiarezza dall'analisi del sistema statunitense di regolamentazione della *privacy* in *Internet*, prevalentemente consegnato a forme di *Self-Regulation*.

L'autoregolamentazione è caratterizzata dall'adozione, da parte delle imprese, di pratiche comuni in materia di tutela della *privacy*, rese note agli utenti mediante l'utilizzo dei cosiddetti « marchi di qualità » o « *seals* »[21]. Questa operazione si basa sulla formazione di documenti operativi, i « *seals programs* », concordati tra le aziende del settore commerciale e le istituzioni che promuovono la tutela della riservatezza. Lo scopo è quello di assicurare determinati *standards* di protezione, all'interno di un sistema in grado di verificare che l'azienda si conformi alle regole del *seal program* e che osservi i comportamenti in tal modo prescritti[22].

La certificazione, però, non è una garanzia assoluta di protezione dei dati e l'utilizzo dei *seals* non ha ottenuto i risultati sperati: in particolare, essa difetta di regole uniformi all'interno dei vari *seal programs* e di un apparato di controllo in grado di assicurare una piena osservanza delle prescrizioni adottate. Le norme predisposte dall'autodisciplina, infatti, sono continuamente soggette a modifica, spesso anche in momenti successivi alla raccolta delle informazioni personali e la loro applicazione è, di regola, esclusivamente volontaria[23]. Spesso, è accaduto che l'utente sia

[21] Cfr. S.F. Bonetti, *La tutela dei consumatori nei contratti gratuiti di accesso ad Internet: i contratti dei consumatori e la privacy tra fattispecie giuridiche e modelli contrattuali italiani e statunitensi*, in questa *Rivista*, 2002, 1120 ss.

[22] Tra i maggiori programmi di certificazione è necessario ricordare *TRUSTe e Better Business Bureau Online*. La prima è un'organizzazione *no-profit* creata dalla *Commercenet and Electronic Frontier Foundation*, ed è da anni impegnata nel diffondere, nel settore dell'industria digitale, procedure operative fondate sui principi di rispetto della *privacy*. A tal fine fornisce alle imprese che operano sul *web*, programmi di gestione costruiti sulla base delle direttive e delle *policies* comunemente accettate in materia di *privacy*. Quanto alla seconda i suoi programmi di tutela includono « *verification, monitoring and review, consumer dispute resolution, a compliance seal, enforcement mechanisms and an educational component* ». Vedi in proposito quanto affermato dal *Council of Better Business Bureau, Inc., About the privacy program*, reperibile sul sito www.bbbonline.org.

[23] Cfr. B.K. Groemminger, *Personal privacy on the Internet: should it be a Cyberspace entitlement?, 36 Ind. L. Rev.* 827 (2003).

stato tratto in inganno dalla visualizzazione di un logo non corrispondente ad un *seal* autorizzato o che, nonostante l'esposizione del marchio, il *seal program* non abbia assicurato lo *standard* di tutela che egli era convinto di trovare[24]. È stato, dunque, attribuito all'utente l'onere di controllare l'effettività dei livelli di protezione dei marchi, all'interno di un sistema in cui ogni forma di tutela è stata delegata esclusivamente alle decisioni del singolo[25].

I pericoli connessi ad un approccio di questo tipo sono molti: la discrezionalità dell'utente in merito alla cessione dei propri dati può generare una diffusione incontrollata delle informazioni personali, con il rischio che la circolazione di certe categorie di dati, per esempio quelli sensibili, pregiudichi l'interessato nella sua posizione sociale, politica ed economica[26].

Di fronte a simili problematiche l'approccio « pluridisciplinare » appare una valida alternativa alle richieste di tutela avanzate dagli utenti. Le sue componenti eterogenee (pluralità di fonti normative, presenza di un'Autorità Indipendente, ausilio degli strumenti tecnici) possono trovare applicazione nell'ambito degli strumenti della *Self-Regulation*, determinando la configurazione di un sistema di tutela che rimanga comunque in linea con le tradizioni giuridiche ivi esistenti. L'introduzione di un quadro generale di regole, infatti, potrebbe avvenire attraverso una legge federale, che fornisca i criteri di base per l'adozione delle norme autodisciplinari[27]. In questo modo, sarebbe possibile fornire a tutti un livello minimo e non negoziabile[28] di prote-

[24] Le *privacy policies*, infatti, sono spesso il frutto di decisioni unilaterali prese dalle aziende, in mancanza di un effettivo confronto con i *privacy advocates* e con le esigenze dei consumatori. Accade, dunque, spesso che il marchio garantisca esclusivamente che il sito che lo espone abbia aderito ad un programma di protezione, ma non assicuri che tale politica di tutela della *privacy* corrisponda ad adeguati livelli di protezione.

[25] Cfr. S. RODOTÀ, *Tecnologie e diritti*, Bologna, Il Mulino, 1995, 109.

[26] Cfr. S. RODOTÀ, *ult. op. cit.*, 84.

[27] Di questo scopo partecipano le numerose proposte di legge presentate negli ultimi anni al Congresso, tra cui l'*Online Privacy Protection Act of 2003*[27], la cui approvazione potrebbe avere un profondo impatto nei confronti della regolamentazione della *privacy* in Rete. Al suo interno, infatti, viene proposto un sistema di protezione dei « *privacy rights* » degli utenti, attraverso la determinazione di precise regole per la raccolta e la diffusione dei dati personali e la previa acquisizione del consenso dell'interessato. Inoltre, viene imposta agli *Internet Service Providers* l'adozione di misure di sicurezza che garantiscano la confidenzialità e l'integrità delle informazioni raccolte e l'applicazione dell'intera disciplina è affidata ai poteri della *Federal Trade Commission*. L'*Online Privacy Protection Act of 2003*, è stato presentato il 7 Gennaio 2003 alla *House of Rappresentative* da Mr. Frelinghuysen, su richiesta della *FTC*. Vedi *Online Privacy Protection Act of 2003, 108th Congress., H.R. 69*. Al vaglio del Congresso inoltre troviamo anche il « *Wireless Privacy Protection Act of 2001* », che introduce un criterio di *opt-in* simile a quello adottato dalle direttive europee; il « *Location Privacy Protection Act* », che impone obblighi di informativa nei confronti degli utenti e prevede la richiesta di un'autorizzazione degli interessati nel caso di comunicazione a terzi dei dati raccolti; infine, il « *Freedom from Behavioral Profiling Act* », che si propone di emendare il *Gram-Leach-Bliley Financial Modernization Act* al fine di rendere le sue previsioni più stringenti. Tutti i testi sono reperibili sul sito *http://Thomas.loc.gov/*.

[28] A tal proposito è necessario ricordare la Convenzione di Strasburgo n. 108 del 1981, al cui preambolo si ravvisa la necessità di una normativa internazionale che « concilii, i valori fondamentali del rispetto della vita privata e della libera circolazione delle informazioni tra i popoli ». Cfr. E. GIANNANTONIO, *Commento all'art.*

zione della *privacy* in *Internet*, attraverso norme applicabili a tutti i trattamenti[29].

Il problema relativo alla mancanza di un'Autorità Indipendente, a sua volta, potrebbe essere affrontato nell'ambito della stessa struttura privata, a prescindere dalla configurazione di un'*Authority ad hoc* sul modello dei Garanti Europei. La necessità di vigilare sul rispetto delle norme dell'autodisciplina potrebbe, infatti, essere risolta all'interno degli stessi *seal programs*, mediante il rafforzamento dei poteri di vigilanza e di supervisione di cui già in parte dispongono le società di gestione dei marchi[30]. Questa attività dovrebbe avvenire sotto il controllo della *Federal Trade Commission*, sulla base dei poteri di vigilanza ad essa attribuiti[31] nei confronti delle imprese nordamericane che hanno aderito al *Safe Harbor Agreement* con l'Unione Europea[32].

In questo modo, si pongono le premesse per la configurazione di una *Self-Regulation* « mutata », proponendo una disciplina in grado di « correggere » i limiti del sistema di protezione fino ad ora adottato. L'approccio « pluridisciplinare » si porrebbe, così, quale naturale evoluzione dell'attuale sistema di autoregolamentazione, producendo effetti positivi sia in termini di protezione della *privacy* in Rete, sia in termini di sviluppo del commercio elettronico[33]. La presenza al suo interno di elementi di « *Strict* » e di « *Self* » *Regulation*, infatti, ha il pregio di renderlo flessibile, in grado di interpretare le esigenze di regolamentazione della circolazione dei dati personali e capace di garantire una maggiore protezione dei diritti degli utenti.

1, *comma I*, in E. GIANNANTONIO, M.G. LOSANO e V. ZENO-ZENCOVICH (a cura di), *La tutela dei dati personali Commentario alla L. 675/1996*, cit., 2 e cfr. C.M. BIANCA, *Note introduttive*, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La tutela dei dati personali. Commentario alla l. 675/96*, cit., 220 ss.

[29] Cfr. K. ALBOUKREK, *Adapting to a new world of e-commerce: the need for uniform consumer protection in the international electronic marketplace*, *35 Geo. Wash. Int'l L. Rev.* 425 (2003).

[30] In questo modo, sarà possibile garantire una « *effective self-regulation* », attraverso la presenza di un organo indipendente e l'individuazione di appropriati meccanismi di *enforcement* delle regole autodisciplinari. In questo senso si è più volte espressa la *Federal Trade Commission*, facendo intendere che la mancanza di un organo di tutela potrebbe vanificare l'effettività delle *privacy policies* adottate dalle imprese. Cfr. G.Y. SATO, *Should Congress regulate cyberspace?*, in 20 *Hastings Comm. Ent. Journ.*, 1998, 699 ss.

[31] Le imprese che abbiano intenzione di aderire all'accordo « *Safe Harbor* », infatti, sono tenute a notificarne l'adesione alla *Federal Trade Commission*, la quale ha il compito di controllare il rispetto delle previsioni dell'accordo e ha il potere di infliggere sanzioni in caso di inadempimento.

[32] L'accordo « *Safe Harbor* » è stato raggiunto dopo due anni di negoziato, con la decisione della Commissione Europea, adottata il 26 luglio 2000. Esso mira ad assicurare ai cittadini dei paesi europei, i cui dati personali siano trasferiti oltreoceano, un livello di tutela adeguato, anche se non equivalente, a quello attualmente previsto nei paesi dell'Unione. Cfr. E. SHAPIRO, *All is not fair in the privacy trade: the Safe Harbor Agreement and the World Trade Organization*, *71 Fordham L. Rev.* 2781 (2003). Cfr. D.A. TALLMAN, *Financial Institutions and the Safe Harbor Agreement: securing cross-border financial data flows*, *34 Law & Pol'y Int'l Bus* 747 (2003).

[33] Il simultaneo intervento di fonti legislative e di norme autodisciplinari, infatti, andrebbe ad esclusivo vantaggio degli utenti e della fiducia che essi ripongono nel Web. La mancanza di riservatezza in *Internet* è divenuta un motivo frenante per la diffusione del commercio elettronico ed una politica a vantaggio della *privacy* degli utenti produrrebbe effetti positivi anche sugli stessi operatori economici. Vedi in proposito il « *FTC Releases Report on Consumer Protection in the Global E-Commerce Marketplace* », adottato dalla *FTC* il 6 Settembre, 2000.

La presenza di così evidenti vantaggi, però, non aiuta a rendere la sua attuazione nel sistema statunitense meno difficoltosa. Malgrado le crescenti richieste di cambiamento, infatti, i tempi non si mostrano ancora maturi per un mutamento di posizione. In Europa, invece, la situazione si presenta diversa: la recente adozione in Italia del Codice della *Privacy* pare volta a cogliere gli aspetti fondamentali dell'approccio « pluridisciplinare » appena descritto, ponendo le premesse per una sua prima applicazione.

3. L'approccio pluridisciplinare introdotto dal T.U. in materia di protezione dei dati personali.

L'approccio « pluridisciplinare » di protezione della *privacy* in Rete si caratterizza per la presenza di una molteplicità di fattori tra loro poco omogenei: una struttura legislativa, l'intervento di norme d'autoregolamentazione, i poteri di controllo di un'Autorità Indipendente ed il supporto delle tecnologie informatiche.

Questo orientamento traspare con evidenza dal recente Codice della *Privacy*[34], approvato con D.Lgs. n. 196 del 30 giugno 2003. Qui, il recepimento della direttiva 2002/58/CE è avvenuto in prospettiva del nuovo modo di concepire la tutela dei dati personali in *Internet*, attraverso la valorizzazione delle forme di autodisciplina ed il rafforzamento dei poteri del Garante.

La parte VII del T.U., infatti, subordina la regolamentazione dell'intera materia alla sottoscrizione del Codice deontologico dei fornitori dei servizi di comunicazione elettronica[35]. Il cambiamento di prospettiva rispetto alle previsioni della direttiva 2002/58/CE è notevole: l'art. 122, 2º comma del T.U., demanda alle norme di buona condotta il compito di individuare i presupposti e i limiti entro i quali il trattamento via *Internet* dei dati personali sia consentito, nell'ottica di una totale subordinazione della legittimità del trattamento al rispetto delle regole predisposte in via autodisciplinare[36].

Il quadro di riferimento così prospettato è quello di un « sistema normativo complesso », caratterizzato dalla presenza di fonti disciplinari differenti e tra di loro in rapporto di interdipendenza reciproca[37].

---

[34] Il Codice assume le caratteristiche di un T.U., riunendo in un singolo contesto la L. 675/96 ed i vari interventi normativi seguiti all'approvazione di quest'ultima. Lo scopo è quello di razionalizzare le norme esistenti, tenendo conto dei più recenti orientamenti della giurisprudenza del Garante. Cfr. M. de Bernart, *Ed ora anche la normativa sulla privacy avrà il suo Testo Unico*, in *Dir. e Gius.*, n. 30, 2003, 81 ss.; cfr. R. Acciai, *Il diritto alla protezione dei dati personali: la disciplina sulla privacy alla luce del nuovo Codice*, cit. Per un commento al Codice, articolo per articolo, cfr. *Il Codice della Privacy*, in *Guida al diritto*, dossier n. 8, 2003.

[35] Con maggiore precisione si tratta di « fornitori » dei servizi di comunicazione ed informazione consistenti « prevalentemente o esclusivamente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i sevizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'art. 2, lett. *c*), della direttiva 2002/21/CE ». Cfr. S. Vigliar, *Privacy e comunicazioni elettroniche: la direttiva 2002/58/CE*, in questa *Rivista*, 2003, 404 ss.

[36] Cfr. G. Busia, *Deontologia parametro di liceità delle operazioni*, in *Guida al dir.*, dossier n. 8, 2003, 150.

[37] Cfr. F. Neumann, *Lo stato democratico e lo stato autoritario*, Il Mulino, Bologna, 1973, 245 ss.

Le norme di carattere legislativo svolgono la funzione di chiarire e differenziare i valori giuridici in gioco, ancorandone il rispetto alla previsione di adeguate sanzioni. In tal modo esse individuano le regole generali e i livelli di protezione, demandando agli strumenti dell'autoregolamentazione il compito di attuarli in concreto.

La *Self-Regulation*, a sua volta, contribuisce alla formazione di una disciplina specifica[38], capace di adattarsi in modo più diretto alle peculiarità della Rete[39]. Essa ha il vantaggio di coinvolgere i fornitori dei servizi di comunicazione elettronica nella predisposizione degli strumenti di tutela a favore degli utenti, in tal modo rispondendo ad una politica di allocazione delle responsabilità, nei confronti dei soggetti che sono in grado di evitare i danni da illegittimo trattamento dei dati. La crescente invadenza degli strumenti elettronici, infatti, ha reso palese l'impossibilità per il singolo di ottenere protezione dagli strumenti attribuitigli in via generale dalla legge[40], rendendo necessario un intervento volto ad una maggiore responsabilizzazione degli operatori del settore[41].

Da questa combinazione di fonti normative emerge una tutela di tipo organico, all'interno della quale l'intervento « pubblico », di carattere legislativo, e gli strumenti « privati », di tipo deontologico, contribuiscono a sviluppare un sistema di protezione della *privacy*, in grado di assicurare un'effettiva protezione dell'utente della Rete.

A partecipare del rapporto di « interdipendenza » tra fonti è anche l'istituzione del Garante, cui è riservato il potere di promuovere i codici di buona condotta e di verificarne la conformità alla normativa in materia. L'Autorità è chiamata a decidere in ultima istanza sul contenuto del codice deontologico, a verificare quali soggetti abbiano titolo per partecipare alla sua elaborazione ed a contribuire, attraverso la redazione di opportune osservazioni, all'approvazione delle norme che lo compongono. In senso favorevole, dunque, deve essere letto il processo di rafforzamento delle sue prerogative effettuato dal Testo Unico: *in primis*, l'ampia funzione nomofilattica che viene affidata al Garante e che fa dei suoi atti, una fonte normativa di rango secondario[42].

Infine, non può essere trascurato il contributo offerto dagli strumenti tecnologici, soprattutto se adeguati alle esigenze della *privacy* in Rete[43].

---

[38] Le norme di buona condotta dovranno continuamente conformarsi alle previsioni di legge, poiché da esse traggono legittimazione. La previsione dei codici deontologici, infatti, non ha le caratteristiche di una vera e propria *deregulation*, per cui la disciplina del settore non viene interamente devoluta all'autonomia dei privati. Cfr. A. Simoncini, *Il sistema delle fonti normative*, in V. Cuffaro e V. Ricciuto (a cura di), *Il trattamento dei dati personali. Vol. II: profili applicativi*, cit., 31.

[39] Cfr. C. Lacava, *Commento all'art. 31*, in C.M. Bianca, F.D. Busnelli (a cura di), *Tutela della privacy*, *Commentario*, cit., 711.

[40] Quali il consenso preventivo dell'interessato, l'informativa, i diritti di accesso, di rettifica, di aggiornamento, di cancellazione dei dati ecc. Cfr. C. Lo Surdo, *Gli strumenti di tutela del soggetto « interessato » nella legge e nella sua concreta attuazione*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, cit., 600 ss.

[41] Cfr. F. Casarosa, *Innovazione e continuità nei codici deontologici e/o di buona condotta* ex *art. 20 del D.Lgs. 467/01: il caso del marketing diretto*, in questa *Rivista*, 2002, 851.

[42] Cfr. R. e R. Imperiali, *Taglia il traguardo l'atteso Testo Unico della privacy*, in *Dir. prat. Soc.*, 2003, n. 14/15, 7.

[43] Vedi in proposito quanto previsto all'art. 3 del T.U. Cfr. C. Filippi, *Principi*

In questo senso sono andate le prescrizioni del D.Lgs. n. 196/2003, che hanno rafforzato, in un quadro di evoluzione tecnologica, le misure di sicurezza contro i rischi di distruzione, intrusione o uso improprio dei dati[44].

4. (*Segue*). Il ruolo delle informazioni da fornire all'interessato.

Il nuovo approccio di tutela della *privacy* in Rete, si caratterizza anche per una maggiore attenzione nei confronti delle informazioni che devono essere fornite all'utente. Accanto all'importanza dell'informativa[45], testimoniata dai numerosi interventi[46] del Gruppo di lavoro dei Garanti Europei[47], si è sviluppata l'attenzione verso nuove indicazioni, in grado di mettere in guardia l'interessato dai pericoli connessi all'uso degli strumenti di comunicazione elettronica.

Tale orientamento risultava già dalla Direttiva 2002/58/CE, laddove in tema di misure di sicurezza è stato previsto a carico del fornitore dei servizi di comunicazione elettronica l'obbligo di informare gli utenti dei rischi ad essa connessi e dei rimedi di possibile attuazione[48]. A tal fine è avvenuto un ampliamento degli oneri d'informazione a carico dei titolari, tra i quali è stato aggiunto l'obbligo di richiamare, accanto alle caratteristiche del trattamento, anche i mezzi di « autotutela » a disposizione dell'interessato.

---

generali, in G.P. Cirillo (a cura di), *Il Codice sulla protezione dei dati personali*, Giuffrè Ed., Milano, 2004, 21 ss.

[44] A tal fine sono state aggiunte alle norme già in vigore (password, codici identificativi, antivirus ecc.), ulteriori previsioni quali l'autenticazione informatica, i sistemi di cifratura, le procedure per il ripristino dei dati ecc. Per un commento cfr. L. Beffino, *Documento programmatico entro il 31 marzo*, in *Guida al dir.*, dossier n. 8, 2003, 118 ss. Vedi inoltre la « Guida operativa per redigere il Documento Programmatico sulla Scurezza » ad uso degli operatori delle piccole e medie realtà, reperibile sul sito *www.garanteprivacy.it*.

[45] In proposito cfr. R. Ristuccia, *Commento all'art. 13*, in E. Giannantonio, M.G. Losano, V. Zeno-Zencovich (a cura di), *La tutela dei dati personali. Commentario alla l. 675/96*, cit., 128.

[46] Alla 25ª Conferenza internazionale svoltasi a Sidney il 10-12 Settembre 2003, è stato posto l'accento sull'importanza dell'informativa in materia di protezione dell'utente. In particolare è stato approvato un documento concernente la necessità di migliorare la chiarezza e l'efficacia delle informative rilasciate agli interessati. La risoluzione impegna quasi 40 paesi a mettere a punto un modello *standard* di informativa che, soggetti pubblici e privati, possano utilizzare per fornire le informazioni essenziali sul trattamento, attraverso « un linguaggio semplice, inequivocabile e diretto ». Il testo ufficiale è reperibile sul sito *www.garanteprivacy.it*.

[47] Il gruppo di lavoro è stato istituito dall'articolo 29 della direttiva 95/46/CE. Si tratta dell'organo indipendente di consulenza dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono stabiliti dall'art. 30 della direttiva 95/46/CE.

[48] All'art. 2, 2º comma, infatti, si prevede che « nel caso in cui esista un particolare rischio di violazione della sicurezza della rete, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di informare gli abbonati indicando, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore del servizio, tutti i possibili rimedi, compresi i relativi costi presumibili ». Cfr. G.M. Riccio, *Il consenso dell'interessato al trattamento via Internet dei dati personali*, in Sica e Stanzione (a cura di), *Commercio elettronico e categorie civilistiche*, Giuffrè editore, 2002, 335.

La stessa tendenza traspare dal Testo Unico, che all'art. 131, prevede l'obbligo dei fornitori dei servizi di comunicazione elettronica di informare l'internauta « circa la sussistenza di situazioni che permettano di apprendere in modo non intenzionale il contenuto di comunicazioni o conversazioni da parte di soggetti ad esse estranei ». Non si tratta di indicazioni da inserire nell'informativa, dal momento che nessun riferimento in proposito è presente nella norma, ma di informazioni « ulteriori », che di quest'ultima condividono l'importanza. Del resto, anche lo scopo non è totalmente diverso da quello delle prescrizioni di cui all'art. 13 del T.U.: l'informativa ha da sempre svolto un ruolo essenziale ai fini della legittimità del trattamento, in qualità di strumento in grado di fornire all'interessato le informazioni indispensabili per la formazione di una libera e consapevole manifestazione di volontà[49]. Le « ulteriori informazioni » previste a carico dei fornitori partecipano dello stesso scopo: rendere presente all'utente la probabile perdita di « confidenzialità » della comunicazione, al fine di creare le premesse per un proficuo esercizio dei diritti riconosciutigli dalla legge.

La disposizione dell'art. 131 del T.U., quindi, si inserisce in un sistema di regole di correttezza, volte ad avvisare gli utenti dei pericoli a cui vanno incontro e diretto a stimolare l'utilizzo degli strumenti di *self-help* e l'adesione ai processi di autoregolamentazione in atto.

Tali motivi partecipano chiaramente del cambiamento in tema di tutela della riservatezza in *Internet*, evidenziando un'esigenza nuova, finalizzata a coinvolgere i fornitori dei servizi della Rete nel compito, sino ad ora di esclusiva prerogativa del Garante, di formare una « coscienza collettiva sul tema della *privacy*[50] ». Il fine è quello dell'acquisizione da parte del singolo di una piena consapevolezza dell'ambito di tutela dei propri dati personali, che gli permetta di sfruttare al meglio i diritti riconosciutigli dalla legge e gli strumenti di protezione a sua disposizione.

5. Il consenso dell'interessato nel sistema di tutela introdotto dal codice deontologico dei fornitori dei servizi di comunicazione elettronica.

L'attuazione della nuova forma di tutela introdotta dal T.U. impone un'attenta riflessione in ordine al consenso dell'interessato e al ruolo che esso dovrà svolgere in prospettiva della sottoscrizione del codice di deontologia previsto ai sensi dell'art. 133.

All'interno del quadro normativo fino ad ora adottato, infatti, il consenso ha assunto un'importanza centrale ai fini della liceità del trattamento, ponendosi come strumento principale di controllo dell'attività di elaborazione dei dati personali. In particolare, esso è divenuto strumento

[49] La mancanza dell'informativa o la inesattezza della stessa, infatti, invalidano il consenso, rendendo illegittimo l'intero trattamento. Vedi la decisione del 28 maggio 1997 del Garante per la Protezione dei Dati Personali.

[50] Tra i compiti del Garante il T.U. riconosce anche una funzione « promozionale », che si manifesta nell'esigenza di diffondere tra il pubblico la conoscenza delle norme che regolano la materia dei dati personali. Cfr. Lacava C., *Commento all'art. 31*, in C.M. Bianca, F.D. Busnelli (a cura di), *Tutela della privacy*, *Commentario*, cit., 713.

di espressione del diritto all'autodeterminazione dell'individuo, sulla base di una nozione di *privacy* quale potere di conoscere, di controllare e di indirizzare il flusso delle informazioni personali[51].

La centralità in tal modo attribuita all'istituto subisce non poche incrinature nell'ambito del nuovo processo di regolazione a cui è improntato il Testo Unico. In particolare, essa si scontra con le problematiche connesse alla rapidità della comunicazione in Rete e con la necessità di attuare le regole attraverso gli strumenti dell'autodisciplina.

Scopo del processo di regolazione della *privacy* in *Internet* è quello di assicurare un livello di protezione dell'utente, che gli permetta di muoversi nella Rete senza preoccuparsi delle tracce lasciate durante la navigazione. A tal fine, è possibile immaginare un sistema di tutela che si esplichi in più livelli, diversificati a seconda delle preferenze espresse dagli utenti. Tale gradazione dovrà partire da un livello minimo, che assicuri un tipo non negoziabile di tutela, attraverso un trattamento dei dati personali limitato al tempo necessario alla trasmissione della comunicazione elettronica. In questa fase, la legittimità del trattamento sarebbe espressione dei principi di cui agli artt. 11 e 3 del T.U., rendendo superflua l'acquisizione del preventivo consenso dell'interessato.

L'art. 11 riconosce i principi di liceità, correttezza e finalità della raccolta[52], nell'ottica di una loro applicazione congiunta[53]. L'art. 3 impone di ridurre al minimo[54] l'uso di dati personali, e individua quale possibile scopo di un livello minimo di tutela, quello di un trattamento effettuato per la trasmissione della comunicazione elettronica. Dalla « correlazione » di questi principi si deduce la formazione di un grado primario, elementare di tutela, costituito dalla realizzazione di trattamenti effettuati in maniera lecita, nel rispetto del principio di correttezza e per scopi strettamente connessi alla trasmissione della comunicazione. Questa fase dovrebbe essere garantita dal Codice deontologico, attraverso un impegno dei fornitori dei servizi *web* al rispetto dei requisiti minimi così individuati. In questo quadro, la preventiva richiesta del consenso non appare necessaria, rimanendo piuttosto d'intralcio alla navigazione. Tale affermazione trae giustificazione dal clima di « ridimensionamento » dello strumento del consenso, reso palese dai recenti interventi normativi in tema di poteri del Garante[55].

---

[51] Si tratta delle informazioni « in uscita » e « in entrata » dalla sfera privata dell'interessato. Il diritto ad essere lasciati soli si è, infatti, esteso a diritto ad essere lasciati in pace, come dimostra l'importanza crescente assunta dal diritto di non sapere, ovvero dall'attribuzione ai singoli del potere di rifiutare interferenze nella loro sfera privata. Per rendersi conto dell'entità del problema è sufficiente pensare alla pratica dello *spamming*. Cfr. M. ATELLI, *Dal diritto ad essere lasciati soli al diritto ad essere lasciati in pace: la prospettiva del danno da petulanza*, in *Riv. crit. dir. priv.*, 1997, 623.

[52] Cfr. E. NAVARRETTA, *Commento all'art. 9*, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *Tutela della privacy*, *Commentario*, cit., 322.

[53] Si è parlato in tal senso di « principio di correlazione », la cui applicazione consente « di identificare gli esatti limiti dell'attività del titolare che integri in qualche modo una compressione della *privacy* dell'interessato ». Cfr. M. GAGLIARDI, *Trattamento dei dati personali e principio di correlazione nel settore assicurativo*, in *Dan. e Resp.*, 2001, 669 ss.

[54] In proposito si è parlato anche di « principio di minimizzazione ». Cfr. R. e R. IMPERIALI, *Taglia il traguardo l'atteso Testo Unico della privacy*, cit., 7.

[55] In particolare si fa riferimento al potere dell'Autorità di decidere in ordine a determinati trattamenti anche in senso

L'acquisizione dello stesso, dunque, si sposterebbbe ad un momento successivo, laddove vengano concepiti livelli ulteriori di tutele, adottati dagli utenti su base volontaria. In questi casi il consenso si fa strumento per la creazione di canali di comunicazione con i consumatori, nell'ottica di attività di commercializzazione attivate su loro richiesta. L'utente passa, così, per gradi, da un rapporto fondato sull'interesse ad un rapporto basato sulla fiducia: con il crescere di quest'ultima, l'interessato viene convinto ad autorizzare una gamma sempre più ampia di attività di trattamento, rivelando una quantità progressivamente maggiore di dati e acconsentendo all'invio di messaggi pubblicitari relativi a nuovi prodotti e servizi[56].

La presenza di una diversificazione dei livelli di protezione introduce all'utilizzo dei cosiddetti « marchi di qualità », capaci di attestare le differenti gradazioni di protezione e variabili a seconda degli scopi del trattamento e del tipo di dati richiesti all'utente. La presenza del marchio garantirebbe all'interessato il rispetto delle condizioni previste dall'informativa rilasciata al momento della richiesta del consenso, mettendogli a disposizione un rapido ed efficace strumento di controllo[57]. Esso inoltre, renderebbe più rapida l'attività di supervisione del Garante, fornendo dei parametri di riferimento ai quali confrontare gli *standards* di tutela effettivamente adottati dai fornitori dei servizi di comunicazione elettronica. Ne risulta un sistema, in cui tra i fornitori dei servizi interattivi si andrebbe a sviluppare una forte attività di « concorrenza », ai fini della fidelizzazione degli utenti sul mercato[58]. La competizione degli *Internet Service Providers*[59] andrebbe, così, ad esclusivo vantaggio di una maggiore protezione della *privacy* in Rete, in un modello in cui il consenso, lungi da essere unico presupposto di liceità del trattamento, diventa strumento, fra i tanti, di realizzazione della tutela.

Non bisogna, inoltre, dimenticare che la nuova lettera *g*) dell'art. 24 del T.U. ha previsto la possibilità per il Garante di determinare, nel rispetto dei principi sanciti dalla legge, l'esclusione del consenso dell'interessato nell'ipotesi in cui il trattamento risulti necessario per il perseguimento di

---

contrario rispetto alla volontà dell'interessato. È quanto avviene in rapporto ai « dati sensibili », ma è anche quanto recentemente previsto all'art. 17, in ordine al trattamento di dati « particolari », ed all'art. 24, lett. *g*) in merito ai trattamenti in cui prevalga un « legittimo interesse del titolare o di un terzo destinatario dei dati ».

[56] Tutto questo andrebbe anche a vantaggio dei fornitori dei servizi, che disporrebbero di informazioni esatte, attuali e più rispondenti alle preferenze degli utenti, limitando i rischi connessi alla cosiddetta « spersonalizzazione » della rete. Cfr. F. Di Ciommo, *Diritti della personalità tra media tradizionali e avvento di Internet*, in G. Comandé (a cura di), *Persona e tutele giuridiche*, cit., 44 ss.

[57] Il marchio, in questo caso, rafforza la funzione di controllo del rispetto dei requisiti di legittimità del trattamento, propria dell'informativa. Esso, infatti, assume le caratteristiche di un « regolamento », delimitando l'ambito di rilevanza dei poteri del titolare e fissando i confini entro i quali il suo comportamento risulti corretto. Cfr. G. Comandè, *Commento agli artt. 11-12*, in E. Giannantonio, M.G. Losano, V. Zeno-Zencovich (a cura di), *La tutela dei dati personali. Commentario alla l. 675/96*, cit., 137.

[58] Cfr. G. Comandé, *Gestori radio-tv ancorati a modelli di condotta*, in *Guida al dir.*, dossier n. 8, 2002, 136.

[59] Gli *Internet Service Providers (ISP)* sono gli operatori professionali che consentono agli utenti di accedere *on-line* ai servizi e alle risorse disponibili nel *Web*. Sull'argomento cfr. F. Di Ciommo, *Evoluzione tecnologica e regole di responsabilità civile*, cit., 259 ss.

« un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato[60] ». In tal modo è stato attribuito al Garante[61] il potere di ritenere legittimi, anche contro la volontà dell'interessato, trattamenti che siano strumentali al soddisfacimento di un interesse di natura economico-patrimoniale del titolare o di un terzo destinatario delle informazioni[62]. Il potere così attribuito all'Autorità si inserisce pienamente nel clima di cambiamento introdotto dalle nuove regole, rispondendo alle intenzioni di un legislatore che, nel tentativo di approntare un sistema di protezione efficace per la sfera personale dell'interessato, considera lo strumento del consenso un elemento centrale ma non indispensabile al raggiungimento della tutela.

6. Alcune applicazioni concrete: l'invio legittimo dei cookies.

Al di là della configurazione del livello minimo di tutela, di fronte ad attività di trattamento operate in relazione al preventivo consenso dell'interessato, il Codice dovrà prevedere anche le regole a cui i fornitori dei servizi *Internet* dovranno sottostare per evitare il perpetuarsi di illegittime invasioni della *privacy* dell'utente. In proposito, il T.U. individua due situazioni precise, costituite dall'invio dei *cookies* e dal fenomeno delle comunicazioni commerciali non sollecitate.

In ordine alla prima ipotesi, l'art. 122, 2º comma del Testo Unico prevede che l'invio dei *cookies* sia consentito per « determinati scopi legittimi » e sulla base del preventivo « consenso informato » dell'interessato. L'attività di specificazione dell'autoregolamentazione dovrà, quindi, avvenire nell'ottica di queste due previsioni di legge, secondo la necessaria conformazione ai parametri di legittimità da questa individuati. La discrezionalità lasciata alle norme dell'autodisciplina, infatti, trova un limite nelle previsioni di rango legislativo, soprattutto in vista del giudizio di conformità espresso dal Garante. Da una parte, l'ammissibilità del marcatore viene subordinata allo scopo per il quale esso è utilizzato, nell'ottica dell'individuazione di un « principio di correlazione[63] » nel campo delle comu-

[60] Tale integrazione si deve all'art. 5, 2º comma del D.Lgs. 467/2001. Cfr. S. Sica, *D.Lgs. n. 467/01 e riforma della privacy: un vulnus al sistema della riservatezza*, in questa *Rivista*, 2002, 363 ss.

[61] Parimenti il legislatore ha esteso la tutela dei dati « particolari », mediante l'ampliamento delle possibilità d'intervento del Garante nei confronti del trattamento di qualsivoglia tipologia di dati che presentino « rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato ». Vedi in proposito quanto previsto dall'art. 17 del T.U.

[62] Tale operazione avverrà in seguito ad un giudizio comparativo tra l'interesse perseguito dal titolare (o dal terzo destinatario) e la posizione dell'interessato. Giudizio destinato a risolversi nel senso della prevalenza della posizione dell'interessato ogni qualvolta il conflitto e la comparazione si instaurino tra « un interesse di natura economico-patrimoniale del titolare (o del terzo) ed i diritti, le libertà fondamentali o la dignità dell'interessato »; il problema rimane, invece, aperto laddove anche la posizione fatta valere da quest'ultimo abbia natura patrimoniale. Cfr. A. Orestano, *La circolazione dei dati personali*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, cit., 165.

[63] Cfr. M. Gagliardi, *Trattamento dei dati personali e principio di correlazione nel settore assicurativo*, cit., 669 ss.

nicazioni elettroniche. Dall'altra, essa dovrà tener conto del rispetto del principio del consenso e delle conseguenze ad esso collegate.

Le regole del codice dovranno, quindi, individuare le ipotesi in cui il *cookie* possa definirsi inviato per « fini legittimi ». Qui la materia è lasciata alla discrezionalità degli operatori della Rete, che terranno presente quanto previsto dalla direttiva 2002/58/CE[64], ma potranno anche includervi situazioni ulteriori. Inoltre, le regole di « buona condotta » dovranno guardare al principio del consenso, facendo attenzione ai requisiti che lo caratterizzano. In proposito è utile ricordare che la parte VII del T.U. si inserisce nel contesto normativo dell'intero decreto, e che, di conseguenza, ad essa si applicano tutte le norme generali previste da quest'ultimo. Il consenso prescritto dagli artt. 122 e ss. è quindi il consenso espresso, libero, informato, specifico e documentato per iscritto, così come previsto dall'art. 23 del Testo Unico[65]. In questo senso il marcatore, sebbene inviato per scopi legittimi, potrebbe non soddisfare il principio del consenso libero. Il rifiuto del *cookie*, infatti, potrebbe avere come conseguenza l'impossibilità di accedere al sito, costringendo l'utente ad accettarne la presenza per non perdere la possibilità di procedere nella navigazione. Il Codice, dunque, dovrà circoscrivere i casi di limitazione dell'accesso al sito, alle sole ipotesi in cui l'invio del *cookie* sia indispensabile alla realizzazione del servizio richiesto dall'utente[66], come quando il *cookie* sia necessario all'accertamento della sua identità[67].

7. (*Segue*): Le comunicazioni non sollecitate.

Analoga problematica si pone in merito alle comunicazioni indesiderate, in ordine alle quali i parametri di riferimento predisposti dalla legge comprendono, oltre alle norme del T.U., anche le previsioni del D.Lgs. 9 aprile 2003 n. 70, che ha recepito la Direttiva 2000/31/CE sul commercio elettronico[68].

In questo caso, a differenza della disciplina relativa ai *cookies*, l'ambito di intervento dell'autoregolamentazione si inserisce nel contesto di previ-

[64] Quest'ultima, al 25° considerando, precisa che i *cookies* possono rappresentare uno strumento legittimo quando sono utili alla verifica dell'efficace progettazione del sito o della corretta impostazione della pubblicità in esso presente. Sempre la Direttiva individua la legittimità di tali dispositivi anche « quando siano destinati a facilitare la fornitura di servizi della società dell'informazione » come nei casi di registrazioni *on-line* o di richiesta di personalizzazione dei siti da parte dell'utente.

[65] All'art. 23 viene previsto che « Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato. (...) Il consenso è validamente prestato solo se espresso liberamente e specificatamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'art. 13 ».

[66] Cfr. S. Patti, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. Dir. civ.*, 1999, 460.

[67] Cfr. G. Cassano e M. Equino, *Il trattamento dei dati personali alla luce della direttiva 2002/58/CE*, in *I contratti*, n. 4, 2003, 411.

[68] Al suo interno, infatti, si prevede che la comunicazione sia identificata in « maniera chiara ed inequivocabile », ovvero che risulti in maniera specifica la tipologia pubblicitaria o commerciale del messaggio. Cfr. M. Dona e E. Quagliato, *Il decreto sul commercio elettronico, un inestricabile groviglio normativo*, in *Dir. e Gius.*, n. 17, 2003, 74 ss.

sioni di legge molto dettagliate. Ai sensi dell'art. 130 del T.U., infatti, l'invio di *e-mails*[69] « a fini di comunicazione commerciale, vendita diretta, invio di materiale pubblicitario » viene subordinato al previo consenso dell'utente. Tale principio subisce una deroga al 4° comma, laddove si precisa che nell'ambito di un preesistente rapporto di clientela, è ammesso l'uso delle coordinate elettroniche dei clienti per finalità di *direct marketing*, a condizione che le informazioni siano state raccolte nel rispetto della normativa a tutela dei dati personali[70]. Questa eccezione è giustificata dal fatto che l'acquisizione delle coordinate elettroniche deve avvenire nel « contesto di vendita di un bene o servizio » e deve riguardare prodotti « analoghi » a quelli precedentemente venduti[71].

È in questo campo che la generalità della norma legislativa dovrà essere sostituita dai parametri più specifici dell'autoregolamentazione. In questo senso sarà necessario precisare il rapporto di connessione oggettiva richiesto tra i prodotti e servizi pubblicizzati e quelli precedentemente acquistati. In particolare, le norme autodisciplinari dovranno specificare il significato da attribuire al termine « analoghi », che dovrà essere interpretato in maniera restrittiva, onde evitare la commercializzazione di tutta la gamma di beni o prodotti disponibili[72].

Infine, è necessario ricordare che la disciplina relativa alle comunicazioni commerciali non sollecitate troverà una regolamentazione più dettagliata all'interno del codice deontologico previsto all'art. 140[73] del T.U. In questo senso le norme dei due codici saranno di arricchimento reciproco, nell'ottica di un coordinamento di tutte le disposizioni dettate in materia[74].

---

[69] La disposizione in realtà si applica anche alle comunicazioni effettuate tramite telefax, messaggi del tipo *Mms* (*Multimedia Messaging Service*) o *Sms* (*Short Message Service*) o di altro tipo. Vedi il Parere del Garante del 10 Giugno 2003, reperibile sul sito www.garanteprivacy.it.

[70] Si tratta d un'importante apertura a favore di un mercato che intende sempre più avvalersi delle comunicazioni elettroniche per la commercializzazione di beni e servizi. Cfr. R. IMPERIALI e R. IMPERIALI, *Comunicazioni elettroniche: la CE impone maggiore tutela della privacy*, in *Dir. prat. soc.*, n. 19, 2002, 35.

[71] Cfr., A. PRADELLA, *Comunicazioni elettroniche*, in G.P. CIRILLO (a cura di), *Il Codice sulla protezione dei dati personali*, cit., 460 ss.

[72] Così, per esempio, di fronte ad una precedente relazione contrattuale tra l'utente e l'impresa di telefonia mobile per la fornitura di una scheda telefonica prepagata, potranno essere legittime le offerte relative ai servizi a pagamento dei quali l'utente può usufruire attraverso la scheda, come quelli relativi agli aggiornamenti sul traffico o al servizio di ricezione delle chiamata all'estero, ma non potranno anche essere pubblicizzate offerte relative alla vendita di telefoni cellulari.

[73] L'art. 140 infatti risponde alla previsione dell'art. 20 del D.Lgs. n. 460/2001, relativo alla sottoscrizione da parte degli organismi rappresentativi del settore, di un codice di deontologia riguardante il trattamento di dati personali, effettuato « ai fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione elettronica ». Cfr. A. SALVI, *La disciplina delle comunicazioni elettroniche non richieste alla luce del D.Lgs. n. 70/2003 sul commercio elettronico e del nuovo « Codice in Materia di protezione dei dati personali »*, in questa *Rivista*, 2003, 1101 ss.

[74] In proposito cfr. l'*Opinion* 5/2004 *on « Unsolicited communications for marketing purposes »*, adottata dal Gruppo di lavoro dei Garanti Europei il 27 Febbraio 2004, WP 90 (11601/EN). Reperibile sul sito www.*europa.eu.int/comm/internal_-market/privacy/workingroup_en.htm*.

8. Brevi riflessioni conclusive.

Alla luce delle considerazioni esposte, l'evoluzione normativa dell'intera materia appare consegnata all'adozione di un approccio « pluridisciplinare » di tutela della *privacy* in *Internet*.

Questo modello è in grado di sostituirsi alla palese insufficienza delle forme di tutela individuale[75], contrapponendosi ad un sistema, in cui l'interferenza nella sfera personale dei cittadini, ha assunto una dimensione difficilmente controllabile da parte degli strumenti civilistici tradizionalmente adottati[76].

L'approccio « pluridisciplinare », inoltre, offre il vantaggio di richiedere comuni sistemi di azione, a prescindere dalle tecniche di applicazione concreta che saranno individuate nello specifico. Ai singoli paesi vengono così lasciati ampi margini di discrezionalità, che rendono possibile il graduale adattamento dei diversi ordinamenti alle nuove esigenze della *privacy* in Rete e l'individuazione di soluzioni compatibili con gli strumenti di regolamentazione cui essi sono abituati.

In questo modo, il raggiungimento di un pari livello di protezione dei dati personali, viene ottenuto all'interno di soluzioni applicative differenti. Così, nell'ambito del sistema europeo, l'approccio « pluridisciplinare » riesce bene ad accordarsi con il principio di tutela della persona e del meccanismo di *opt-in*. Tutto questo è testimoniato dalle previsioni del recente Codice della *Privacy*, in cui l'intervento autoregolamentare viene inserito nella struttura di tutela improntata ai principi del consenso dell'interessato e della trasparenza delle attività di trattamento.

A sua volta, nell'ottica del sistema statunitense, l'approccio organico di protezione diviene elemento capace di adattarsi alla tradizione giuridica ad esso appartenente, inquadrandosi nel contesto dei *seals* e delle strutture di *Self-Regulation*.

Questa situazione rende possibile la configurazione di un modello internazionale di tutela, in cui la circolazione delle informazioni personali avvenga tra paesi che hanno raggiunto un comune livello di protezione. L'adozione dell'approccio « pluridisciplinare », infatti, permette la creazione di *standards* adeguati di tutela dei dati, nel rispetto delle tradizioni giuridiche di ogni ordinamento e degli strumenti applicativi che esso voglia adottare. In questo modo, la realizzazione di un effettiva tutela, potrebbe avvenire senza eccessivi sconvolgimenti delle caratteristiche di ogni singola tradizione giuridica. La diversità dei modelli, dunque, lungi dal pregiudicare il dialogo tra i paesi, produrrebbe effetti vantaggiosi per tutti, determinando lo sviluppo di una più « sicura » circolazione delle informazioni, in grado di costituire un passo determinante nel processo di riconoscimento internazionale di un diritto alla protezione dei dati personali.

---

[75] Cfr. C. Camardi, *Mercato delle informazioni e privacy. Riflessioni generali sulla L. n. 675/96*, in *Eur. e dir. priv.*, 1998, 1060.

[76] In questa situazione di pericolo diventa indispensabile adottare delle strategie integrate di protezione, in cui l'intervento di fonti di disciplina autoregolamentare si affianchi alle norme di legge ed all'attività di controllo di un'Autorità Indipendente.