RENATO CLARIZIA

LEGGE 675/96 E RESPONSABILITÀ CIVILE

SOMMARIO: Premessa. — 1. La ricognizione dei principali articoli della legge 675/96 nei quali sia possibile individuare l'eventuale fonte di responsabilità civile a carico dei soggetti che « trattano » i dati personali. — 2. L'art. 18 e le misure minime di sicurezza. — 3. Trattamento ordinario e i diritti dell'interessato. — 4. Il trattamento « speciale » dei dati sensibili e i diritti dell'interessato. — 5. Conclusioni in tema di responsabilità civile

PREMESSA.

La legge 675/96, come è noto, attua la direttiva comunitaria 95/46/CE del 24 ottobre 1995 « relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati » ed adempie ad obblighi internazionali (quali quelli derivanti dall'accordo di Schengen e dalla Convenzione del Consiglio d'Europa sulla « Protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale » conclusa a Strasburgo il 28 gennaio 1981). È evidente dalla lettura della normativa la contrapposizione tra l'interesse del Titolare ad un libero « trattamento » dei dati personali e quello del soggetto al quale i dati si riferiscono (l'« interessato ») ad esercitare un effettivo e continuo controllo. Siffatta contrapposizione si colloca in un più ampio panorama che riguarda in generale la odierna « dimensione » della *privacy* nella società dell'informazione e dell'informatica.

Non è possibile in questa sede svolgere riflessioni su questa tematica, ma il rinvio è d'obbligo ai numerosi saggi di Stefano Rodotà che con la sensibilità e lungimiranza che gli sono consuete, con la finezza di grande Giurista che lo contraddistinguono, con

* L'articolo — che riproduce il testo della relazione tenuta al Congresso di Pesaro del 27 febbraio 1998 su *Privacy e responsabilità dell'impresa* — è destinato agli studi in onore di Sergio Antonelli.

la chiarezza espositiva che coniuga perfettamente il rigore scientifico con la concretezza delle soluzioni proposte, ha evidenziato le peculiarità, i pericoli, i vantaggi del progresso tecnologico nella società contemporanea e l'incidenza (di rilevanza non solo giuridica) sulla nozione di *privacy*. Ecco come Egli riassume gli « effetti sociali delle tecnologie dell'informazione e della comunicazione » sulla *privacy*: « siamo passati da un mondo in cui le informazioni personali erano sostanzialmente sotto il controllo esclusivo degli interessati a un mondo di informazioni condivise con una pluralità di soggetti; siamo passati da un mondo in cui la cessione delle informazioni era nella gran parte dei casi l'effetto di relazioni interpersonali, sì che la forma corrente di violazione della *privacy* era il pettegolezzo, a un mondo in cui la raccolta delle informazioni avviene attraverso transazioni astratte;

— siamo passati da un mondo in cui il solo problema era quello del controllo del flusso delle informazioni in uscita dall'interno della sfera privata verso l'esterno ad un mondo nel quale diventa sempre più importante il controllo delle informazioni in entrata, come dimostra l'importanza crescente assunta dal diritto di non sapere, dall'attribuzione ai singoli del potere di rifiutare interferenze nella loro sfera privata come quelle derivanti dall'invio di materiale pubblicitario e dal *marketing* diretto;

— viviamo in un mondo nel quale cresce il valore aggiunto delle informazioni personali, con un cambiamento di paradigma, dove il riferimento al valore in sé della persona e alla sua dignità diviene secondario rispetto alla trasformazione dell'informazione in merce;

— viviamo in un mondo in cui si sta acquistando la consapevolezza di riflettere sul fatto che, finora, le tecnologie dell'informazione e della comunicazione hanno troppo spesso assunto i caratteri di tecnologie sporche, avvicinandosi piuttosto al modello delle tecnologie industriali inquinanti, sì che diventa centrale favorire o imporre l'introduzione nell'ambiente informativo di tecnologie pulite;

— viviamo in un mondo — conclude Rodotà — in cui proprio le tecnologie dell'informazione e della comunicazione hanno contribuito a rendere sempre più labile il confine tra sfera pubblica e sfera privata: e la possibilità di una libera costruzione della sfera privata e d'uno sviluppo autonomo della personalità sono diventate condizioni per determinare l'effettività e l'ampiezza della libertà nella sfera pubblica. » (RODOTÀ, *Tecnopolitica*, Bari 1997, p. 151).

Ho riportato testualmente il pensiero di Rodotà, perché è proprio nel contesto sociale e giuridico che Egli così sinteticamente e chiaramente disegna, che viene a collocarsi la legge 675/96 e pertanto questa legge va interpretata, criticata e, se del caso, modificata, tenendo conto di quel contesto. A me sembra che uno dei rilievi critici che possono muoversi alla legge (con un'immediata e diretta ricaduta sul tema della responsabilità civile di cui specificamente mi occuperò) è che essa non è stata capace di staccarsi

completamente dal « vecchio » sistema per disciplinare la materia in maniera del tutto « nuova ». Si pensi, ad esempio, al continuo ricorso alla scrittura quale forma che devono rivestire gli atti riguardanti il trattamento dei dati personali (prevalentemente svolto informaticamente), soprattutto il consenso che deve prestare l'interessato e che costituisce un po' il fulcro dell'intera disciplina.

Assunta consapevolezza del mutamento della società civile, incapace di offrire al cittadino una tutela della propria *privacy* così come le era stato possibile in passato, la legge avrebbe dovuto correttamente distinguere gli eventi di rilevanza esclusivamente economica da quelli davvero capaci di incidere nella sfera di intimità individuale. Avrebbe dovuto meglio bilanciare la varietà di adempimenti e oneri a carico del Titolare e il « potere » attribuito all'interessato di limitare o impedire il trattamento dei dati personali. È evidenza generalizzata il fatto che le incombenze a carico del Titolare sono spesso eccessive e costose, oppure si risolvono in un mero formalismo che non consentono poi all'interessato alcun tipo di controllo « effettivo ». Sicché di fronte a talune prescrizioni della legge 675/96, ci si interroga sulla stessa *ratio* su cui si fondano.

In una tale ottica, a me pare che l'attenzione del legislatore si sarebbe dovuta concentrare da un lato sulla tutela dei dati sensibili e di quelli concernenti la salute — non trascurando peraltro di tenere in giusta considerazione anche le legittime pretese del medico nel rivendicare una certa autonomia decisionale nel rapporto col paziente, ad esempio sul se dire o no la verità sulla malattia — dall'altro sulla richiesta di consenso unicamente per quei trattamenti tesi ad ottenere risultati ultronei e diversi rispetto a quelli manifestati al momento della raccolta.

Non deve sottacersi, però, che, di fronte ai problemi nuovi posti dalla società dell'informazione e dell'informatica, e quindi di fronte alla necessità di offrire ai cittadini gli strumenti giuridici adeguati per affermare i propri diritti di opposizione ad indiscriminate forme di raccolta e di circolazione delle informazioni personali, per affermare il « diritto di non sapere » (soprattutto con riguardo ai dati sulla salute), per affermare il diritto a conoscere e a vigilare sul rispetto delle finalità della raccolta, per affermare ancora il diritto all'oblio di quelle informazioni personali che hanno già attuato le finalità per cui furono raccolte, di fronte insomma a problemi di così ampia portata e rilevanza, la risposta del legislatore non poteva essere subito apprezzata unanimemente e rispondere a tutte le esigenze della società.

L'auspicio è che sotto l'accorta guida di Rodotà, nella sua veste di Garante, si possano apportare le opportune modifiche ed integrazioni alla normativa vigente anche in quelle parti attinenti ai profili della responsabilità civile sui quali mi soffermerò tra breve.

Premetto che la mia indagine è focalizzata esclusivamente a situazioni nelle quali Titolare è un'impresa privata.

1. La ricognizione dei principali articoli della legge 675/96 nei quali sia possibile individuare l'eventuale fonte di responsabilità civile a carico dei soggetti che « trattano » i dati personali.

Tra gli interrogativi che con maggiore insistenza si sta ponendo la dottrina che affronta le problematiche, varie e complesse, suscitate dalla legge 675/96 (e dai provvedimenti emanati dal Garante), quello fondamentale mi pare riguardi quale sia l'obiettivo di fondo perseguito dalla normativa: la disciplina della circolazione delle informazioni, la disciplina dei dati personali o la tutela della persona. Soltanto la risposta chiara ed inequivocabile al suddetto quesito può orientare correttamente il giurista nella sua attività interpretativa e quindi anche nella concreta rilevazione delle ipotesi in cui sia individuabile una responsabilità (civile o penale) in capo ai soggetti che « trattano » i dati personali. Il titolo della legge indirizza indubbiamente l'interprete a leggerla in chiave di individuazione dell'ambito di riservatezza, di *privacy*, di cui ancora gode oggi il cittadino; ma a me sembra che sostanzialmente la normativa si preoccupi soprattutto di regolamentare la circolazione delle informazioni personali: quando esse possano essere considerate di dominio pubblico, quando ne possa essere impedita la circolazione, quando se ne possa ottenere una circolazione limitata.

È, dunque, al momento della circolazione dell'informazione personale che il legislatore presta principalmente attenzione, soprattutto tenendo conto del suo trattamento in via informatica. Ed è difatti ad eventi in qualche modo legati alla « circolazione » delle informazioni personali che hanno attinenza le principali fattispecie normative di responsabilità (civile) del titolare contemplate dalla legge e che richiamo velocemente di seguito.

L'art. 7 disciplina il contenuto e le modalità della notificazione che « il titolare che intenda procedere a un trattamento di dati personali soggetto al campo di applicazione della presente legge è tenuto » a fare al Garante.

L'art. 8.1 prescrive che il Responsabile preposto dal Titolare sia nominato « tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza ». L'art. 8.2 prevede che il Titolare dia le opportune istruzioni al Responsabile e vigili « sulla puntuale osservanza delle disposizioni di cui al comma 1 e delle proprie istruzioni ». L'art. 8.5 prevede che sia il Titolare o il Responsabile a dare adeguate istruzioni agli incaricati del trattamento.

L'art. 9 si sofferma sulla qualità del trattamento e della raccolta dei dati personali.

L'art. 10 specifica il contenuto dell'informativa che deve essere data all'interessato.

L'art. 11, nel condizionare la legittimità del trattamento — e solo per inciso ricordo la grande ampiezza di significato che l'art.

1.2 lett. *b*) attribuisce al termine « trattamento » — alla prestazione del consenso dell'interessato, al terzo comma sottolinea che « il consenso è validamente prestato solo se e espresso liberamente in forma specifica e documentata per iscritto e se sono state rese all'interessato le informazioni di cui all'art. 10 ».

L'art. 12 elenca i casi nei quali il Titolare non è tenuto a chiedere il consenso per il trattamento.

L'art. 13 elenca i diritti che l'interessato può far valere nei confronti del Titolare, imponendogli determinate modalità di trattamento dei dati personali o inibendogli il trattamento stesso. Il terzo comma prevede che se i dati personali si riferiscono a persone decedute, i diritti « possono essere esercitati da chiunque vi abbia interesse ».

L'art. 15 si occupa delle misure di sicurezza che devono essere adottate per custodire i dati personali oggetto di trattamento.

L'art. 18 richiama l'art. 2050 cod. civ. quale parametro di riferimento nella valutazione del danno che deve essere risarcito da « chiunque cagiona danno ad altri per effetto del trattamento di dati personali ».

Così come l'art. 9 tratta della raccolta dei dati personali, gli artt. 20 e 21 si soffermano rispettivamente sui casi in cui la comunicazione e la diffusione dei dati personali siano consentite e vietate.

Infine, gli artt. 22 e 23 concernono il trattamento dei dati sensibili e di quelli attinenti alla salute, mentre l'art. 29.9 precisa che la risarcibilità del danno non patrimoniale è possibile anche nel caso di violazione delle prescrizioni dell'art. 9, che tratta delle modalità della raccolta e di come devono essere « tenuti » i dati.

A questo punto, possiamo già tentare di individuare, dalla suddetta rapida ricognizione delle principali norme interessanti la responsabilità (civile), gli orientamenti del legislatore che, mi sembra, guardano in tre direzioni: salvo che sia fatto a fini esclusivamente personali, di ogni trattamento deve essere data analitica e puntuale informazione all'interessato; salvo che si rientri nei casi specificamente previsti di esclusione (art. 12), ogni trattamento di dati personali deve essere autorizzato dall'interessato; se il dato oggetto del trattamento rientra tra quelli ccdd sensibili è prevista una regolamentazione ancora più garantista per l'interessato. Nell'ambito di queste tre direttrici e dei relativi adempimenti che incombono sul Titolare e/o sul Responsabile, è possibile individuare quali siano le fattispecie di responsabilità (civile) in capo ai suddetti soggetti.

2. L'ART. 18 E LE MISURE MINIME DI SICUREZZA.

L'art. 18 della legge 675/96 recita testualmente che « chiunque cagiona danni ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile ».

(Che prevede: « Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di aver adottato tutte le misure idonee a evitare il danno »).

Trattasi, dunque, di un'ipotesi di responsabilità oggettiva, in cui la prova liberatoria consiste nella dimostrazione che i dati sono stati trattati — e cioè raccolti, registrati, organizzati, conservati, elaborati, modificati, selezionati, estratti, raffrontati, utilizzati, interconnessi, bloccati, comunicati, diffusi, cancellati e distrutti — secondo le tecniche più avanzate del momento e precipuamente orientate ad evitare l'insorgere di eventi dannosi per l'interessato. Non è dunque sufficiente « la prova negativa di non aver commesso alcuna violazione delle norme di legge o di comune prudenza, ma occorre quella positiva di aver impiegato ogni cura o misura atta ad impedire l'evento dannoso » (Cass. 20 luglio 1993, n. 8069). Anzi, la stessa « prova del caso fortuito, della forza maggiore e del fatto del danneggiato o del terzo può raggiungere effetti liberatori soltanto se escluda, in modo certo, il nesso causale tra l'attività pericolosa e l'evento, non già quando questi elementi possano aver concorso alla produzione del danno, inserendosi in una situazione di pericolo, che ne abbia reso possibile l'insorgenza, a causa dell'inidoneità delle misure preventive adottate. » (Cass. 9 maggio 1967, n. 934).

Inoltre, rileva ancora la suprema Corte che « una volta accertato il nesso causale tra il verificarsi del danno e la mancata adozione di misure di sicurezza da parte dell'esercente un'attività pericolosa, è irrilevante, ai fini dell'esclusione della responsabilità ex art. 2050 c.c., che il danneggiato non abbia sopperito con autonome iniziative, alle omissioni imputabili al gestore dell'attività medesima; l'art. 2050 c.c., infatti, non pone obblighi di diligenza a carico dei terzi estranei alla gestione dell'impresa pericolosa, né limita il proprio ambito operativo alle ipotesi in cui la pericolosità sia occulta, non avvertibile secondo un metro di ordinaria diligenza e quindi tale da tradursi in una insidia nascosta » (Cass. 29 maggio 1989, n. 2584).

Questo rapido quadro giurisprudenziale manifesta chiaramente che la previsione dell'art. 18 della legge 675/96 pone a carico di colui che tratta il dato personale oneri operativi di difficile definizione e di generica prevedibilità, tanto più che — fatti salvi quei soggetti che hanno come oggetto sociale proprio una o più delle attività contemplate dalla legge nella definizione di « trattamento » di cui all'art. 1.2 lett. *b*) della legge 675/96 — il trattamento del dato personale costituisce un qualcosa di « ordinario », « necessariamente » collegato all'attività svolta. È ovvio, infatti, che ogni impresa ha dipendenti, fornitori, clienti, ecc. e può dunque sembrare effettivamente eccessivo l'aver considerato il « trattamento » nel suo insieme « attività pericolosa » e non invece solo taluni specifici profili (ad esempio, l'adozione delle misure di sicurezza ai fini della conservazione). Se si pensa che siffatti adempimenti,

per non incorrere nella previsione dell'art. 18, fanno carico a tutti i soggetti, grandi e piccoli, più o meno organizzati, con attività lucrative e non, si comprende bene che il loro impatto può risultare davvero traumatico.

Proviamo a esplicitare la portata dell'art. 18 avendo riguardo all'approntamento delle misure minime di sicurezza di cui all'art. 15, il cui primo comma dispone che i dati personali « devono essere custoditi e controllati... in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta », mentre il secondo comma precisa che le misure minime di sicurezza saranno dettate con d.P.R.. Quindi: ridurre al minimo i rischi e misure minime di sicurezza, secondo le indicazioni dell'art. 15; tutte le misure idonee ad evitare il danno, secondo l'art. 18. I due articoli non indicano criteri di valutazione omogenei dell'idoneità delle misure di sicurezza adottate e ciò sicuramente complica dal punto di vista interpretativo, anche perché su questo punto il legislatore italiano si è discostato dalla normativa della direttiva, il cui art. 17 prevede che « le misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere ». Ecco, « i costi dell'applicazione » da un lato — l'art. 6 della legge tedesca 27 gennaio 1977 prescrive che vi debba essere una certa proporzionalità tra le spese da affrontare per la sicurezza e il bene da tutelare — e « la natura dei dati da proteggere » dall'altro, sono due criteri che non sono affatto presi in considerazione dal legislatore italiano. A mio parere, invece, sarebbe stato opportuno introdurre anche nel nostro sistema un criterio di proporzionalità, per quanto riguarda i costi, perché l'esigenza di rispettare il dettato dell'art. 18 — e cioè adottare « tutte le misure idonee ad evitare il danno » — non sempre può trovare adeguata soddisfazione proprio in ragione dei costi da affrontare, che potrebbero rivelarsi eccessivi e sproporzionati rispetto alle dimensioni dell'impresa, alla natura dei dati personali da trattare e/o alle finalità del trattamento.

La protezione dei diritti di libertà e di dignità della persona che non possono né devono essere sacrificati al cospetto delle grandi banche dati (soprattutto informatiche) non può nemmeno però avere sempre e comunque il sopravvento sui diritti (anch'essi costituzionalmente garantiti) di iniziativa economica.

3. Trattamento ordinario e diritti dell'interessato.

La legge 675/96 elenca una serie di situazioni giuridiche soggettive che fanno capo all'interessato — qualificabili in termini di di-

ritti soggettivi — e che hanno ad oggetto il trattamento dei dati personali.

Innanzitutto, l'interessato ha diritto ad essere informato analiticamente sul trattamento dei propri dati personali: l'informativa non è dovuta solo qualora il Garante ritenga l'impiego dei mezzi necessari per l'informativa « manifestamente sproporzionato rispetto al diritto tutelato » o la stessa impossibile, oppure se il trattamento dei dati avvenga ai fini dello svolgimento di investigazioni per la difesa giudiziaria in sede penale o civile (art. 10, 4° comma). Egli ha diritto a sapere le finalità e le modalità, la natura obbligatoria o facoltativa del conferimento dei dati, le conseguenze del rifiuto di rispondere, l'ambito soggettivo di comunicazione e diffusione dei dati, i diritti che gli sono attribuiti dall'art. 13, i dati identificativi del Titolare e del Responsabile. Il legislatore ritiene, correttamente, che soltanto una trasparente e puntuale esposizione delle attività che il Titolare intende svolgere sui dati personali di cui dispone possano poi mettere in grado l'interessato di dare un consenso consapevole al loro trattamento. Ne consegue, pertanto, l'emersione di responsabilità se l'informativa fosse vaga, di difficile comprensione, reticente, parziale, non veritiera. Peraltro anche l'art. 9.1, lett. *b*), si preoccupa di evidenziare che i dati personali oggetto di trattamento devono essere raccolti e registrati per scopi « espliciti ».

In particolare, devono essere chiaramente indicati le finalità e l'ambito della comunicazione e diffusione dei dati. L'accertamento dell'effettivo rispetto o meno di quanto indicato nell'informativa consentirà di valutare la sussistenza o meno di responsabilità civile a carico del Titolare e/o del trasgressore.

All'interessato è conferito il diritto di esprimere il proprio consenso al trattamento, fatti salvi quei casi di esclusione, elencati nell'art. 12 e che attengono: alla raccolta in base ad un obbligo legislativo, regolamentare o in ragione di una norma comunitaria; all'esecuzione del contratto o alle trattative precontrattuali in cui è parte l'interessato; all'estrazione da registri o da documenti pubblici; ad attività scientifiche o di statistica e se sono dati anonimi; all'attività giornalistica, pur nel rispetto di certe regole; al segreto aziendale e industriale; a situazioni incidenti sulla salvaguardia della vita e dell'incolumità fisica dell'interessato; allo svolgimento, infine, di investigazioni per la difesa giudiziaria in sede penale o civile. Il mancato consenso può essere foriero di conseguenze negative anche per l'interessato e di ciò egli deve essere informato. È bene però rilevare che le conseguenze del mancato consenso non devono essere sproporzionate rispetto al trattamento inibito: il cliente che neghi all'impresa che fornisce periodicamente certi beni o servizi il trattamento dei propri dati personali a fini di pubblicità non può sentirsi opporre quale conseguenza del rifiuto il recesso dal contratto. Il consenso, infatti, deve essere non soltanto consapevole ed informato, ma anche « espresso liberamente »; è ovvio che la prospettazione

di ingiustificate gravi conseguenze per la mancata prestazione del consenso costituisce un (nemmeno tanto!) occulto modo per forzare la volontà dell'interessato, e come tale può essere fonte di responsabilità civile. Anzi, tanto è vero che il consenso deve essere prestato liberamente che si richiede che i modelli di consenso siano predisposti, anche da un punto di vista grafico, in modo che siffatta libertà sia evidente (ad esempio, scrivendo « consento » « non consento » e spiegando che l'interessato deve porre una *ics* accanto al testo che preferisce) e non invece prevedendo che il consenso formi già il contenuto di una clausola a stampa.

Ovviamente — e lo si è già messo in evidenza prima — la prestazione del consenso è strettamente collegata ad una corretta informativa: il consenso è infatti dato con riferimento a quello specifico trattamento esplicitato nell'informativa che non può quindi essere generica ed indeterminata. D'altra parte anche tutti gli altri diritti di cui è titolare l'interessato presuppongono — come vedremo — una corretta informativa, che costituisce, pertanto, il nucleo centrale dell'intera normativa.

Ai sensi dell'art. 9, inoltre, l'interessato ha diritto alla qualità dei dati, nel senso che essi devono essere trattati correttamente e lecitamente, quindi « raccolti e registrati per scopi determinati, espliciti e legittimi », aggiornati, corretti e pertinenti rispetto agli scopi dichiarati. Essi devono essere conservati soltanto per il periodo strettamente necessari al trattamento.

Siffatto diritto inerisce alla tutela della propria identità personale, qualità individuale che riguarda intimamente l'interessato e alla cui « formazione » contribuiscono sia la verità e completezza dei dati che lo riguardano sia l'esistenza di taluni dati e non di altri. Ecco perché è a tal riguardo importante non soltanto l'informativa (devo sapere quali dati che mi riguardano sono stati raccolti e sono trattati) ma anche la prestazione consapevole e cosciente del consenso (perché volendo dare una certa « immagine » di me consento il trattamento solo di alcuni dati oppure posso denunciare la incongruità del trattamento di determinati dati rispetto alle finalità indicate nell'informativa). Il controllo sulla qualità del dato personale costituisce perciò uno dei momenti principali di affermazione e di tutela della personalità individuale rispetto alla ormai generalizzata aggressione dei mezzi informatici e quindi all'inevitabile venir meno del diritto alla riservatezza nella dimensione di un tempo.

In sostanza, se è vero che oggi non è più possibile difendere la propria *privacy*, posso però pretendere di controllare i dati che mi riguardano. Sicché connessi strettamente a questo diritto sono anche quelli alla cancellazione dei dati e alla rettifica. Il primo, contemplato dall'art. 13.2, lett. *c*) n. 2, consente all'interessato di ottenere « la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge » o quando la loro conservazione non è necessaria in relazione ai fini per i quali sono stati

raccolti e trattati. In tal modo viene affermato il cd diritto all'oblio, che assume evidentemente nella società informatica un'importanza basilare, forse uno degli ultimi baluardi della *privacy*.

Siffatto profilo della normativa deve essere tenuto in grande considerazione perché concerne il diritto del Titolare a conservare archivi; diritto che deve essere « autorizzato » dall'interessato.

Il diritto alla rettifica si risolve, nella previsione dell'art. 13.1, lett. *c*), n. 3), nel potere attribuito all'interessato di ottenere « l'aggiornamento, la rettificazione ovvero, qualora vi abbia interesse, l'integrazione dei dati ». In tal caso, dunque, il controllo sui dati da parte dell'interessato è finalizzato alla formazione e conservazione del dato personale « corretto ». È legittimo chiedersi se spetti all'interessato oltre che il diritto di chiedere la cancellazione del proprio dato personale anche quello alla sua rettificazione e permanenza nella banca dati. Ad esempio, a fronte della volontà del Titolare di non voler procedere alla rettificazione e/o all'aggiornamento del dato personale, bensì alla sua cancellazione, può l'interessato chiederne la rettificazione e la conservazione? A me sembra che, essendo il trattamento del dato personale finalizzato al soddisfacimento di un interesse del Titolare, spetti a quest'ultimo deciderne la sopravvivenza o meno, salvo che l'interessato non provi di avere un autonomo diritto a chiederne la conservazione (ad esempio anche solo in ossequio all'art. 2058 c.c.), e cioè l'ipotesi della reintegrazione in forma specifica.

I suddetti diritti sono in un certo qual modo connessi e conseguenti al riconoscimento a favore dell'interessato sia del diritto di accesso gratuito al registro generale dei trattamenti tenuto dal Garante (art. 13, 1° comma, lett. *a*)), sia di poter conoscere l'identità del Titolare e del Responsabile del trattamento, nonché le finalità e le modalità del trattamento; nonché, ai sensi dell'art. 13, 1° comma n. 1, di ottenere dal Titolare o dal Responsabile la conferma sull'esistenza dei dati personali e la loro comunicazione in forma intelligibile. Si conferma, dunque, l'orientamento che ormai caratterizza dal punto di vista giuridico la società informatica. Acquisita la consapevolezza che non è possibile frenare il progresso tecnologico e preso atto della caduta di tutti quei veli che ancora riuscivano a salvaguardare una certa *privacy*, il legislatore si preoccupa di disciplinare compiutamente il diritto di accesso a quei dati, perché solo in questo modo si riesce ancora a garantire un certo dominio dell'interessato sui dati personali che lo riguardano.

Altro diritto che compete all'interessato è quello, previsto all'art. 13, 1° comma, lett. *d*) « di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta », diritto di cui la previsione della successiva lettera *e*) — riguardante l'invio di materiale pubblicitario e il cd *direct marketing* — costituisce una particolare specificazione.

La genericità della formula adoperata dal legislatore italiano — « per motivi legittimi » — diversa da quella recata dalla direttiva comunitaria — « motivi preminenti e legittimi, derivanti dalla sua situazione particolare » — viene di fatto ad investire direttamente il giudice del compito di delimitare l'ambito di operatività del diritto di opposizione e di soppesare di volta in volta i contrapposti interessi in gioco. In verità, la delicatezza di questo profilo della disciplina avrebbe forse giustificato una maggiore analiticità da parte del legislatore e la fissazione di criteri interpretativi, seppure generali.

Il successivo art. 17, 2º comma, individua un'ipotesi di « motivo legittimo » di opposizione al trattamento: quando si voglia adottare una decisione — diversa da un atto amministrativo o giudiziario, anch'essi colpiti nel primo comma dal divieto — (evidentemente sfavorevole per l'interessato) fondata sul trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato.

Infine, è riconosciuto all'interessato il diritto alla sicurezza dei dati, diritto di cui si è già discusso innanzi e che qui si intende richiamare solo per rilevarne l'ampiezza di applicazione. Esso, infatti, può essere fatto valere anche nelle ipotesi che sono escluse dal campo di applicazione della legge: il trattamento dei dati per scopi esclusivamente personali (art. 3), il regime speciale previsto per la pubblica amministrazione (art. 4).

4. Il trattamento « speciale » dei dati sensibili e i diritti dell'interessato.

Sempre nell'ottica dell'impresa Titolare del trattamento, passo ad analizzare la normativa concernente i dati sensibili, disciplina che va ora integrata con il provvedimento 19 novembre 1997, recante « Autorizzazione n. 1/1997 al trattamento dei dati sensibili nei rapporti di lavoro ».

È in particolare l'art. 22 della legge che più ci interessa, in quanto il rapporto di lavoro con i propri dipendenti e/o la specifica attività aziendale (ad esempio la vendita di sedie a rotelle per paraplegici) può comportare il venire a conoscenza, tramite il trattamento del dato personale, dell'origine razziale ed etnica, delle convinzioni religiose, filosofiche, politiche o sindacali, oppure dello stato di salute e/o della vita sessuale dell'interessato. In tal caso, la tutela apprestata dal legislatore è maggiore di quella ordinaria, in quanto, oltre al consenso dell'interessato, è necessaria la previa autorizzazione del Garante. Ed è proprio a tal proposito che il Garante ha rilasciato un'autorizzazione di carattere generale al trattamento dei dati sensibili attinenti ai lavoratori subordinati, ai componenti gli organi interni, ai lavoratori autonomi e a quant'altri abbiano rapporti con l'impresa, quando il trattamento

sia necessario per rispettare obblighi legislativi e regolamentari, ai fini previdenziali, assistenziali, di sicurezza e di salute sui luoghi di lavoro, ecc.. L'autorizzazione generale, che ha validità fino al 30 settembre 1998, non esonera, comunque, dall'obbligo dell'informativa e dall'acquisizione del consenso scritto dell'interessato.

Inoltre, per quei trattamenti che non rientrano tra quelli coperti dall'autorizzazione generale deve ritenersi negata l'autorizzazione da parte del Garante, che nello stesso provvedimento precisa anche che restano fermi i divieti posti dall'art. 8 della legge 300/1970 al datore di lavoro di effettuare indagini sulle opinioni politiche, religiose e sindacali del lavoratore, dall'art. 6 della legge 135/1990 di fare indagini per verificare l'esistenza dello stato di sieropositività e dalla normativa in tema di pari opportunità e di prevenzione dalle discriminazioni.

Soltanto nell'ipotesi che il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale sia necessario al fine dello svolgimento di investigazioni per la difesa in sede civile e penale di « un diritto di rango pari a quello dell'interessato », l'art. 25, 4° comma, richiede la sola previa autorizzazione del Garante e non il consenso dell'interessato.

La disciplina del trattamento dei dati sensibili è senza dubbio uno degli aspetti maggiormente qualificanti l'intera normativa che li regolamenta, considerandosi, ad esempio, lo stato di salute non più in una dimensione individuale ma — come rileva giustamente Alpa — in « una dimensione che interessa la collettività, entro i limiti in cui essa possa apprenderlo o ingerirsene, sempre senza arrecare violazioni alle libertà individuali, alla dignità, alla riservatezza e all'identità personale ». Anzi, è soprattutto con riguardo ai dati sensibili che Alpa evidenzia un « paradosso della *privacy*: se si vuole essere tutelati, occorre disvelarsi, come credente, come propalatore di idee, come orientato sessualmente, come malato, ecc.. Occorre cioè aderire a quei criteri di identificazione, anche se essi non si condividono, anche se sono imposti dalla maggioranza, ecc.. Per i giuristi — prosegue ancora Alpa — si apre il problema del rapporto tra *majority rules* e *minority rights*; ma pure il problema della scelta e della vincolatività dei criteri di identificazione. Nel *panopticon* della società odierna, identità, distinzione, differenza sono affidate a codificazioni che hanno lo scopo di proteggere, piuttosto che non di discriminare; ma la tutela è necessariamente accordata solo in quanto ci si sia omologati a quei criteri distintivi. Chi non si vuol omologare — ed è per certi aspetti (e non per altri) libero nella scelta — accetta un rischio, rinuncia alla difesa apprestatagli dalla comunità, finisce per emarginarsi dal contesto sociale ».

La lucida analisi svolta da Alpa e lo stesso contenuto dell'autorizzazione generale rilasciata dal Garante al trattamento dei dati sensibili da parte delle imprese, di cui si è detto prima, ci porta

a meditare sulla bontà della scelta legislativa di condizionare al consenso dell'interessato il trattamento di questi dati anche quando essi siano strutturalmente integrati e talvolta indissolubilmente connessi alle fasi in cui si svolge il rapporto tra l'interessato e il Titolare. Ciò significa, in sostanza, che per taluni dati, seppure sensibili, perché attinenti ad esempio alla salute, il consenso dell'interessato si risolverà in una mera formalità che provocherà esclusivamente un aggravio in termini temporali e di dispendio di materiale cartaceo! Meglio sarebbe stato, dunque, isolare legislativamente quelle fattispecie che, soprattutto nell'ambito di un rapporto di lavoro subordinato e/o autonomo, prevedono necessariamente — per provvedimento legislativo o regolamentare — il trattamento del dato sensibile; meglio sarebbe stato, proprio al fine di evidenziare quelle situazioni nelle quali, invece, mancando siffatta necessità, debba essere davvero l'interessato a consentirne il trattamento.

5. Conclusioni in tema di responsabilità civile.

Alla fine di questa lunga esposizione della normativa recata dalla legge 675/96 e coinvolgente ipotesi di responsabilità civile dei soggetti che trattano i dati personali, proviamo a sistematizzare siffatte ipotesi.

In estrema sintesi, possiamo considerare distintamente il rapporto che viene a crearsi tra l'interessato ed il Titolare e/o il Responsabile e/o l'Incaricato del trattamento, da un lato e quello tra l'interessato e « chiunque » ponga in essere un'attività che gli provoca danni, dall'altro.

Quanto al primo rapporto, emerge chiaramente che il mancato rispetto dei diritti dell'interessato di cui all'art. 13 della legge costituisce la principale e più ampia previsione di fattispecie causative di danni. Si evidenzia così la centralità dell'informativa che deve essere chiara, completa ed analitica nonché della rispondenza delle iniziative concretamente adottate nel trattamento dei dati personali rispetto a quanto ha formato oggetto dell'informativa e del connesso consenso dell'interessato. Assume in tale contesto una importanza centrale il profilo organizzativo interno, e cioè la necessità che i dati personali siano aggiornati e/o corretti tempestivamente, affinché gli stessi siano sempre « veritieri ». Si pensi ad esempio a quelle banche dati cui hanno accesso vari soggetti e che mi consentono tra l'altro di sapere se un certo nominativo è in regola o meno con i pagamenti: la tempestività dell'aggiornamento serve a dare una visione reale e veritiera e soprattutto la intempestività potrebbe essere fonte di danni.

Allo stesso modo si deve dare adeguata rilevanza al profilo della sicurezza che deve garantire la corretta custodia dei dati, evitando accessi non autorizzati, modifiche e cancellazioni involontarie.

Per quanto riguarda il profilo soggettivo, il tema è complesso e di ampia portata. Oltre, infatti, al Titolare, al Responsabile e all'Incaricato del trattamento, è preso in considerazione « chiunque cagiona danni » e non soltanto all'interessato ma genericamente ad « altri ».

Se, dunque, il Responsabile e l'Incaricato del trattamento potranno esonerarsi dalla responsabilità per i danni provocati, qualora riescano a dimostrare di aver svolto diligentemente e con perizia il trattamento dei dati personali, rispettando fedelmente le istruzioni ricevute, ribaltando, in ultima analisi la responsabilità « esclusivamente » sul Titolare, la previsione dell'art. 18, richiamandosi genericamente a « chiunque » e ponendo come unica prova liberatoria quella « di aver adottato tutte le misure idonee ad evitare il danno », sembrerebbe di fatto sconfessare siffatta « gerarchia ».

A tal proposito, io ritengo che una lettura rispettosa comunque della *ratio* della legge 675/96 impone di interpretare la suddetta norma nel senso che sarebbe prova sufficiente « di aver adottato tutte le misure idonee a evitare il danno » proprio il rispetto delle istruzioni del Titolare e/o del Responsabile, perché è esclusa ogni autonomia decisionale in merito alle modalità di trattamento e alle misure di sicurezza da adottare.

Quanto, infine, all'ambito ed all'ampiezza della responsabilità, certamente la circostanza che legittimato attivo a richiedere il risarcimento dei danni sia « chiunque » e non solo l'interessato, apre una problematica al momento non completamente focalizzabile in tutti i suoi possibili contorni e che, evidentemente, la giurisprudenza sarà chiamata a precisare.

Lo stesso può dirsi per quanto riguarda la risarcibilità del danno morale che, mi sembra, trovi, *prima facie*, la propria diretta e immediata applicabilità quale ipotesi di violazione del diritto (dell'interessato e di altri) alla propria identità personale.

È un tema, dunque, difficile e complesso non soltanto per il giurista chiamato ad interpretare la normativa ed a trovarle una coerente collocazione nel nostro sistema giuridico, ma anche e soprattutto per l'operatore che, prima ancora di attrezzarsi per adeguarsi alla normativa, ne deve comprendere e condividere la *ratio* volta, attraverso la disciplina della circolazione dei dati personali, a realizzare una regolamentazione delle relazioni sociali più consona alla società informatica nella quale viviamo.

Si tratta, perciò, innanzitutto di educare i cittadini ad utilizzare lo strumento informatico nel rispetto dell'altrui identità personale e di salvaguardare quel poco che resta di *privacy* (ormai soprattutto riferita ai ccdd dati sensibili) senza compromessi o cedimenti, riducendo come sempre tutto ad un puro calcolo economico.

È riflessione condivisa da tutti, infatti, che il nostro sistema giuridico, la nostra cultura, a differenza di quella angloamericana, non hanno ancora assunto piena dimestichezza con queste proble-

matiche e la stessa legge 675/96 — benché da più di un decennio fossero stati presentati disegni di legge — avrebbe dovuto avere prima della sua approvazione una pubblicità e diffusione sociale ben più ampia di quella (limitata ai soli addetti ai lavori) che ha avuto, proprio per farne conoscere prima il contenuto ai cittadini ed evitare per quanto possibile quella violenza di impatto che invece ha avuto.

Sono consapevole che quando si scontrano i due opposti interessi di tutela della *privacy* del cittadino e di utilizzazione dell'informatica nell'attività di impresa, non debba necessariamente soccombere quest'ultima; ma neanche si può sacrificare *tout court* (quel che resta del) la riservatezza all'altare del progresso tecnologico e ridurre tutto al puro fatto economico del risarcimento del danno.

È sicuramente nella ricerca di un giusto equilibrio tra i suddetti due opposti interessi che si gioca il futuro della nostra società in questo campo ed è auspicabile che gli interventi del Garante da un lato e la giurisprudenza dall'altro riescano a guidarci con sicurezza al di fuori di quell'incertezza di disciplina che talvolta caratterizza l'applicazione della normativa recata dalla legge 675/96.