INDICE

INTRODUZIONE……pag. 1

CAPITOLO PRIMO – *Origini ed evoluzione storica della privacy*

1.1 Cenni storici sul concetto di privacy……pag. 4

1.2 Le figure affini alla privacy……...pag. 6

1.3 La situazione italiana: il concetto di privacy in Costituzione....pag. 8

1.4 La necessità di una legge sulla protezione dei dati……...pag. 10

1.5 Il contesto europeo di riferimento……..pag. 13

CAPITOLO SECONDO – *Il Garante e la Pubblica Amministrazione*

2.1 Nascita dell'Autorità Garante……....pag. 16

2.2 Compiti del Garante.....pag. 17

2.3 Privacy e PA: una difficile convivenza.....pag. 25

2.4 Il regime differenziato nel trattamento dei dati in ambito pubblico.....pag. 27

2.5 I principi applicabili da parte della PA.....pag. 31

2.6 Le forme di tutela.....pag. 32

2.6.1 Tutela amministrativa

2.6.1.1 Il reclamo.....pag. 33

2.6.1.2 Il ricorso.....pag. 34

2.6.2 Tutela giurisdizionale.....pag. 38

CAPITOLO TERZO – *La PA tra accesso e riservatezza*

3.1 Premessa.....pag. 41

3.2 Il concetto di trasparenza.....pag. 43

3.3 L'accesso.....pag. 46

3.3.1 L'accesso civico.....pag. 48

3.4 I "principi generali" in materia di procedimento amministrativo.....pag. 51

3.5 Il responsabile del procedimento amministrativo e l'attività di partecipazione al procedimento.....pag. 53

CAPITOLO QUARTO – *Il panorama internazionale*

4.1 Premessa: il modello europeo.....pag. 57

4.2 La Francia.....pag. 60

4.2.1 La nuova legge e il caso Google.....pag. 61

4.3 La Spagna.....pag. 62

4.3.1 Archivi pubblici e privati.....pag. 66

4.3.2 L'autorità di controllo.....pag. 68

4.4 La Gran Bretagna: la legge di seconda generazione.....pag. 68

4.4.1 Il sistema normativo.....pag. 69

4.4.2 Il diritto dell'interessato.....pag. 70

4.4.3 Gli obblighi del titolare.....pag. 70

4.4.4 L autorità garanti della protezione dei dati personali.....pag. 71

4.5 Gli Stati Uniti.....pag. 72

CONCLUSIONI.....pag. 75

BIBLIOGRAFIA.....pag. 77

INTRODUZIONE

Il tema della riservatezza nel tempo di internet e dei social network è piuttosto complesso: il confine tra una sfera e l'altra si fa sempre più labile. Sulla rete siamo continuamente raggiunti da una vasta mole di notizie e, se da un lato viviamo questa condizione come una straordinaria opportunità di progresso e di libertà, dall'altro lato soffriamo l'incubo del Big Data e della capillare intrusione nella nostra privacy da parte di terzi[1].

Internet, come qualsiasi strumento, racchiude in sé due elementi contrapposti: se è vero infatti che può scatenare e diffondere comportamenti emulativi pericolosi e drammatici, come la cronaca nera ci ricorda a cadenza pressoché quotidiana, è altrettanto indiscutibile il suo ruolo dirompente nel propagare per esempio le proteste contro regimi dittatoriali, tale da far alimentare la speranza in quei popoli di non vedersi abbandonati. Di fronte ad un mezzo dalle simili potenzialità dovrebbe valere il consiglio "maneggiare con cura".

Foto imbarazzanti, sfoghi e confessioni compromettenti, numeri di carte di credito, indirizzi e contatti telefonici: in rete ormai si trova di tutto, e non perché qualche 007 pagato da un governo o da una fantomatica Spectre lo abbia ordito, ma semplicemente perché ad inserire quei dati, quelle informazioni, sono gli stessi utenti, cioè noi.

Come ha ben sintetizzato Luca De Biase, giornalista del Sole 24 Ore, il dilemma non è più "to be or not to be" ma "to share or not to share", condividere o non condividere. Se non condividi praticamente non esisti, eppure secondo una ricerca del Censis per il 96% degli italiani la riservatezza dei dati personali sarebbe un dato inviolabile tanto che immettere informazioni in rete genererebbe forte apprensione.

Nonostante ciò la stessa ricerca rileva come solo il 40% di chi naviga usa almeno una delle misure di salvaguardia della propria identità digitale, mentre addirittura il 36% non ricorre ad alcuno strumento nonostante la piena consapevolezza che i grandi operatori del web (Google, Facebook, ecc.) possiedano gigantesche banche dati sugli utenti.

I dati personali hanno infatti un grandissimo valore economico e possono essere usati sia a livello commerciale (si pensi alle pubblicità mirate attuate da produttori di beni e servizi ansiosi di raggiungere un target definito e preciso piuttosto che buttare soldi in ormai passate campagne pubblicitarie generiche) sia

[1] Rossotto, R., *La privacy al tempo di internet e social network*, www.diritto24.ilsole24ore.it

politico (per esempio in occasione delle campagne elettorali) e sia per questioni di sicurezza nazionale (si guardi il caso Snowden)[2].

Proprio per essere continuamente minacciata dagli operatori dei media (internet, telefonia, ecc.) e dalla nostra leggerezza, la privacy ha la curiosa caratteristica di essere uno tra i diritti più difficili da definire.

Vista in termini di relazione dell'individuo rispetto alla partecipazione sociale, la privacy è il temporaneo distacco di una persona dalla società in generale attraverso mezzi fisici o psicologici, sia in uno stato di solitudine che nell'intimità di un piccolo gruppo o, nel caso di gruppi più grandi, in una condizione di anonimia o riservatezza.

Dalle parole sopra riportate si ricava che la privacy è dunque il potere (o il diritto) del singolo individuo di avere il controllo sulle informazioni che gli appartengono. Ma quando un'informazione può essere definita tale?

Si potrebbe rispondere: quando la stessa è capace di descrivere, raccontare in modo veritiero alcuni particolari di un certo individuo. Un'informazione, infatti, per sua stessa natura non può appartenere ad alcuno: essa è un veicolo, e null'altro.

Oggi, il problema non è quello di adeguare una nozione nata in altri tempi ad una situazione profondamente mutata, rispettandone le ragioni e la logica d'origine. Volendo decifrare il dibattito in corso, infatti, ci si accorge che in esso non si riflette soltanto il classico tema della difesa della sfera privata contro le invasioni dall'esterno, ma si realizza un importante cambiamento qualitativo, che spinge a considerare i problemi della privacy nell'ambito dell'attuale organizzazione del potere, di cui appunto l'infrastruttura informativa rappresenta ormai una delle componenti fondamentali.

Il presente lavoro mira a far luce su una tematica molto complessa e sempre più attuale. Si organizza in 4 capitoli: nel primo ci si sofferma sull'origine e sull'evoluzione storica del concetto di privacy; nel secondo si definiscono i soggetti preposti al controllo della stessa; il terzo è dedicato al contesto normativo in cui è calata la necessità di tutelare il diritto alla riservatezza; nell'ultimo, infine, è presentata una panoramica internazionale sul concetto di privacy.

[2] Toro, A., *Italiani e privacy nell'era dei social network*, www.unimondo.org

CAPITOLO PRIMO

Origini ed evoluzione storica della privacy

1.1 Cenni storici sul concetto di privacy

"Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano e tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto per legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica". E' quanto sancisce l'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea promulgata il 18 dicembre del 2000. Le origini dei concetti di dato personale, di trattamento del dato, e di privacy, per usare un termine inglese abitualmente accostabile ad astrazioni italiane come "riservatezza" e "privatezza", oggi frequentemente in uso sia nel linguaggio comune che in ambito giuridico e politico, potrebbero dunque sembrare di epoca abbastanza moderna. In realtà, tradizionalmente il concetto di privacy affonda le sue radici dottrinali nella Boston di fine Ottocento.

Tutto ebbe inizio con un saggio apparso il 15 dicembre 1890 sulla Harvard Law Review, "The Right to privacy", opera di due giovani avvocati bostoniani, Samuel D. Warren e Louis D. Brandeis, che non scrivevano contro i paparazzi, i settimanali gossip, la tv trash o i blogger senza volto, ma vissero l'esplosione della stampa quotidiana, e gli inizi del fotogiornalismo, coi resoconti mondani e la curiosità per l'indiscrezione di rango. Furono loro a concepire "the right to be let alone", moderna formula dello "jus solitudinis", e cioè il diritto a essere lasciati soli, per godere in pace della propria vita. Lo fecero con argomenti ancora oggi dirimenti: si fondarono sulla Common law, ma distinsero il diritto alla riservatezza dal diritto di proprietà privata. Invocarono la tutela della sensibilità, frutto del processo di civilizzazione, e la protezione dei sentimenti, delle emozioni e dei pensieri privati, come estensione del diritto alla proprietà privata[3].

Era la formulazione del valore giuridico della sensibilità umana ed è considerata l'architrave teorica che ancora oggi fonda per noi il diritto soggettivo all'inviolabilità della persona, al rispetto per la sfera privata, alla riservatezza sui dati così detti sensibili. Per molti anni comunque le teorie di Warren e Brandeis hanno incontrato le forti resistenze di alcune corti le quali erano pronte a sacrificare l'intimità del privato in nome

[3] Valensise, M., *The right to be let alone*, www.ilfoglio.it

dell'interesse collettivo. A partire dal 1960, da quando cioè un altro giurista, Dean William Prosser, in un saggio sulla California Law Review, sistematizzò il concetto di "Privacy" e la sua violazione attraverso quattro distinte categorie (penetrare in uno spazio chiuso, rivelare in pubblico i fatti privati, mettere qualcuno in cattiva luce o appropriarsi a fini commerciali del nome o dell'immagine di un privato, senza che questi abbia dato il suo consenso), le cose cominciarono davvero a cambiare[4]. Nel 1967 il settimanale Life aveva pubblicato la foto di una casa privata per illustrare la prima di una pièce di teatro fondata su un romanzo di Joseph Hayes, tratto da una storia vera, capitata a una famiglia del Connecticut, presa in ostaggio in casa sua. James Hill, il patriarca tenuto in ostaggio, fece causa al settimanale per invasione della privacy, e ottenne un risarcimento di 75 mila dollari. Vinse pure l'Appello, perché i giudici stabilirono che Life aveva creato "un dispositivo fittizio con intento di pubblicità e a fini commerciali, usando il nome di un privato e della sua famiglia, come base per un thriller tratto dalla vita reale". Fu una vittoria (postuma) di Warren e Brandeis, i quali nel loro saggio del 1890 avevano dimostrato come "l'assenza di malizia in colui che pubblica non può essere invocata a difesa", e nemmeno "la verità del fatto reso pubblico". Perché? Per la semplice ragione che a fondare il risarcimento non è il danno arrecato alla reputazione, bensì la lesione stessa del diritto alla riservatezza, "che implica non solo il diritto a impedire un ritratto impreciso della vita privata, ma qualsiasi discussione intorno ad essa".

1.2 Le figure affini alla privacy

Dall'articolato concetto di privacy, tratto dall'esperienza statunitense, sono in breve derivati tutti i vari adattamenti. Il trapianto infatti non è stato meccanico, automatico, ma ha avuto appunto bisogno dei giusti adattamenti al nuovo sistema giuridico e alle nuove esigenze della società dell'informazione.

In Italia il primo a proporre una teoria dell'interesse al riserbo è stato Ferrara Santamaria, che lo ha definito come "un diritto contro le indiscrezioni e curiosità altrui"[5]: una specie di diritto all'inedito, applicato alla sfera d'intimità della persona, ed escludendo l'ingerenza di estranea conoscibilità e pubblicità, oltre i limiti imposti da ragione di ordine pubblico.

Altri hanno parlato di diritto alla riservatezza e l'hanno definita "come quel modo di essere della persona il quale consiste nella esclusione dell'altrui conoscenza di quanto ha a riferimento la persona medesima"[6].

E' d'immediata evidenza che alcune espressioni costituiscono la traduzione letterale del termine (riservatezza» e «riserbo» sono traduzioni di privacy, «diritto ad essere lasciati soli» corrisponde al («diritto to be let alone») e, in ogni caso, la traduzione letterale non si è sostituita all'uso diffuso e non contestato di privacy. Poiché nel mondo del diritto la terminologia non è mai casuale, ma riflette o il portato della

[4] Valensise, M., op. cit.

[5] Ferrara-Santamaria, *Il diritto alla illesa intimità privata*, in Riv. Dir. Priv., 1937, I, p. 168

[6] De Cupis, *I diritti della personalità*, in Trattato di diritto civile e commerciale, a cura di Cicu, Messineo, continuato da Mengoni, Giuffrè, Milano, 1982. Secondo cui il rifiuto a consentire la conoscenza di informazioni sul proprio conto soddisfa "quel bisogno d'ordine spirituale che consiste nell'esigenza di isolamento morale".

traduzione o il portato delle prassi o le origini straniere, appare evidente che nell'esperienza italiana il diritto alla privacy, inteso in senso moderno, è il frutto di un'importazione dal mondo del *common law*.

Oggi la situazione si è inevitabilmente complicata per la presenza di diverse figure di diritti che si affiancano, si avvicinano o addirittura s'intrecciano con il diritto alla privacy. Ci si riferisce in particolare:

a) al diritto all'immagine, che riguarda l'uso che terzi facciano dell'effige di una persona, sia a scopo informativo e divulgativo, sia scopo economico in senso stretto (in questo caso si parla sempre con terminologia inglese di *right of publicity);*

b) al diritto alla identità personale, cioè all'identità ideale che è costituita dal patrimonio di valori, d'orientamenti politici, economici sociali o sessuali proprio di un individuo e che non deve essere stravolto o distorto nel modo in cui è illustrato al pubblico;

c) al diritto al nome, non più considerato solo come un segno distintivo, ma anche come espressione della storia personale, del modo d'essere e di presentarsi di un individuo;

d) all' identità genetica;

e) ai diritti del malato, quando la malattia è collegata con il comportamento (edonistico, sessuale, ecc.);

f) al conflitto tra questi diritti o più precisamente di queste figure del diritto unitario e onnicomprensivo della personalità, con il diritto di cronaca, proprio dei giornalisti operanti nei quotidiani o nelle reti radiotelevisive e con il diritto d'espressione artistica.

La privacy inoltre interferisce con attività che, per ragioni di evoluzione delle tecnologie, rendono più vulnerabili la persona: è il caso della raccolta, mediante tecnologie informatiche, di banche dati personali; è il caso delle intercettazioni telefoniche; è il caso di notizie e immagini trasmesse via «internet».

L'applicazione del diritto alla privacy ha prima lambito e poi investito settori disparati, assai distanti tra loro, si pensi a settori quali la privacy e l'espressione del voto di un organo collegiale amministrativo, la sanzione di sospensione della patente di circolazione con autoveicoli, le registrazioni raccolte illegittimamente e utilizzate nel corso di un procedimento penale, l'edificabilità dì balconi e palazzi, le perquisizioni dei detenuti, l'installazione di una telecamera nell'atrio e nelle scale di un edificio disposta dal condominio a fini di sicurezza, le foto tramite telefonini, e così via.

La privacy oggi in definitiva può essere considerata un diritto civile, e collocato all'interno dei diritti di terza generazione, dopo e accanto ai diritti politici e i diritti sociali.

1.3 La situazione italiana: il concetto di privacy in Costituzione

La Carta Costituzionale italiana non disciplina espressamente il diritto alla tutela della vita privata in quanto tale. Le ragioni della mancata considerazione risiedono essenzialmente nel fatto che il concetto di privacy ha

assunto rilevanza crescente nell'ambito della scienza giuridica e dell'ordinamento italiano a partire dagli anni '60[7].

Con l'emergere di una nuova sensibilità, la Costituzione, sebbene priva di richiami diretti e di portata generale, ha comunque adeguatamente risposto alle incipienti esigenze di tutela, presentando un insieme di disposizioni che formano un sistema diretto a proteggere il singolo nella sua vita privata.

Tra queste disposizioni, un rilievo fondamentale è assunto dall'art. 2, architrave dell'affermazione del principio c.d. "personalista" (che pone l'individuo al centro dell'ordinamento giuridico), riconoscendo e garantendo i diritti inviolabili dell'uomo. Siffatto riconoscimento si collega, oltre che alla dimensione sociale, anche a quella prettamente individuale (come singolo), ciò fornisce lo spunto per asseverare un ampio riconoscimento della vita privata come valore costituzionale protetto.

A rafforzare ulteriormente questa conclusione si pongono altre disposizioni, che hanno riguardo ad aspetti specifici del prisma rappresentato dalla "vita privata".

In tal senso, giova ricordare la garanzia approntata dall'art. 3, secondo comma, relativa al pieno sviluppo della persona umana, o l'art. 13, che nell'affermare l'inviolabilità della libertà personale garantisce il singolo da ogni indebita ingerenza nella sua sfera fisica e psichica.

L'art. 14, dal canto suo, nel sancire l'inviolabilità del domicilio, attribuisce rango costituzionale al principio secondo cui "my home is my castle", proteggendo così una delle sedi – anzi, la sede per eccellenza – in cui la vita privata si svolge.

Nell'ottica relazionale, di particolare importanza è l'art. 15, ai termini del quale "la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili": la disposizione garantisce l'individuo da ogni intromissione che non trovi giustificazione in esigenze di ordine generale, debitamente vagliate dall'autorità giudiziaria.

In una analoga prospettiva, la tutela della libertà di manifestazione del pensiero, di cui all'art. 21, si pone, in una delle sue articolazioni, a presidio anche della pretesa di non rendere noto ai terzi quanto intimamente connesso al proprio modo di essere.

In definitiva, nonostante altri articoli della Costituzione vadano ad incidere sulla sfera privata (si pensi all'art. 19 che garantisce il diritto di professare la propria fede religiosa), rimane comunque l'art. 2 la cornice entro la quale iscrivere la gran parte delle manifestazioni riconducibili alla vita privata.

Basta dare un'occhiata alla giurisprudenza della Corte: la sentenza n. 38 del 1973 definendo i concetti di decoro, onore, rispettabilità, riservatezza, intimità e reputazione, sancisce un link diretto con gli artt. 2, 3 e 13; oppure la sentenza n. 238 del 1996 ha ribadito che la dignità umana è "comprensiva del diritto alla riservatezza"; o infine, la sentenza n. 467 del 1991, sottolineando il rapporto stretto tra l'art. 21 (libertà di manifestazione dei propri convincimenti morali) e l'art. 19 (fede religiosa), ha rilevato che "la sfera intima della coscienza individuale deve essere considerata come il riflesso giuridico più profondo dell'idea

[7] Bellocci-Magnanensi-Passaglia-Rispoli, *Tutela della vita privata*, Incontro trilaterale delle Corti costituzionali spagnola, portoghese e italiana, Lisbona, 2006.

universale della dignità umana che circonda quei diritti, riflesso giuridico che, nelle sue determinazioni conformi a quell'idea essenziale, esige una tutela equivalente a quella accordata ai menzionati diritti, vale a dire una tutela proporzionata alla priorità assoluta e al carattere fondante ad essi riconosciuti nella scala dei valori espressa dalla Costituzione italiana"[8].

1.4 La necessità di una legge sulla protezione dei dati

A partire dagli anni.'70, gli organi comunitari e internazionali hanno sollecitato gli Stati ad ancorare il trattamento dei dati ad una base giuridica precisa e legata all'evoluzione tecnologica e hanno deplorato l'atteggiamento dei paesi rimasti inerti quali l'Italia.

Consapevole, quindi, della diffusione delle tecniche di comunicazione di massa e della facilità con cui le tecnologie consentono al privato di manovrare le informazioni, il legislatore ha creduto di dover dare una risposta a tutte le istanze sollevate negli ultimi anni, dalla dottrina e dalla giurisprudenza, circa la tutela della persona anche rispetto al trattamento dei dati personali: vale a dire una legge che protegga non già il dato in quanto tale, ma, attraverso la protezione del dato, la persona nella sua unicità.

La legge più importante in materia di riservatezza è la legge 31 dicembre 1996, n. 675, sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, la cui finalità era quella di garantire il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale. E' un testo prodotto al termine dei lavori della Commissione Mirabelli e stabilisce il principio secondo cui i soggetti sottoposti al trattamento devono essere avvisati e delucidati sul fine dell'elaborazione dei propri dati prima ancora che essi vengano elaborati. Prima di questa i riferimenti normativi della *privacy* erano contenuti in testi che se ne occupavano in modo settoriale. Si pensi alla legge 8 aprile 1974, n. 98, espressamente dedicata alla «tutela della riservatezza e della libertà e segretezza delle comunicazioni», che all'art. 1 prevede un nuovo reato, destinato ad essere inserito nel codice penale, così come l'art. 615 bis diretto a punire chiunque, mediante l'uso di ripresa visiva o sonora, "si procura indebitamente notizie o immagini attinenti alla vita privata" di altri.

A questo primo intervento legislativo, circoscritto alla tutela della riservatezza e riferibile esclusivamente ad ipotesi d'illecita acquisizione della notizia o dell'immagine, hanno fatto seguito altre leggi, dirette ad una tutela civile della riservatezza senza postulare un previo accertamento dell'illiceità della condotta che si pone in conflitto con tale tutela.

Chiaramente in funzione di salvaguardia della riservatezza si pongono, inoltre, le norme che dettano limiti in materia d'attestazioni di stato civile: le quali, se riferite, per esempio, a persona della quale sia stata giudizialmente rettificata l'attribuzione di sesso, sono rilasciate con la sola indicazione del nuovo sesso (legge 14 aprile 1982, n. 164, art. 5). Analoga funzione perseguono, infine le norme che pongono limiti alla raccolta d'informazioni e, in particolare, alla costituzione di banche di dati personali: si pensi all'art. 8 della

[8] Bellocci-Magnanensi-Passaglia-Rispoli, op. cit.

legge 20 maggio 1970 n. 300 statuto dei lavoratori che vieta al datore d'indagini anche a mezzo di terzi, sulle opinioni politiche, religiose e sindacali del lavoratore nonché su fatti non rilevanti ai fini dell'attitudine professionale del lavoratore.

Ormai, il fondamento normativo di una tutela civile della riservatezza non poteva più essere disconosciuto.

Dopo la 675/96[9] fu introdotta in Italia una nuova normativa: ispirato all'introduzione di nuove garanzie per i cittadini, alla razionalizzazione delle norme esistenti e alla semplificazione, il testo unico in materia di protezione dei dati personali, definitivamente approvato dal Consiglio dei ministri il 27 giugno del 2003 e denominato "Codice della privacy".

Il provvedimento, sulla base dell'esperienza di 6 anni, riunisce in unico testo, la legge 675/1996 e gli altri decreti legislativi, regolamenti e codici deontologici che si sono succeduti negli anni; contiene importanti innovazioni tenendo conto della "giurisprudenza" del Garante e della direttiva Ue 2002/58 sulla riservatezza nelle comunicazioni elettroniche, il Codice si pone in quest'ottica come uno "Statuto dell'informazione personale".

La struttura del D.lgs 196/2003[10] è organizzata sostanzialmente in tre parti.

La prima comprende le regole generali per il trattamento dei dati privati e pubblici, i diritti dell'interessato, dei soggetti che effettuano il trattamento, il dovere alla sicurezza dei dati unita ad altri adempimenti di varia natura, e ad una regolamentazione sul trasferimento all'estero.

La seconda parte contiene invece disposizioni precise in merito a particolari settori tra cui: giustizia, forze di polizia, sanità, istruzione, trattamenti per fini statistici e scientifici, settore bancario ed assicurativo, reti telematiche, giornalismo, investigazione privata, marketing privato.

La terza ed ultima parte viene interamente dedicata alla tutela dell'interessato e alle modalità con cui è possibile adempiere all'esercizio dei suoi diritti, non che ai compiti del Garante, alla struttura organizzativa dello stesso Garante, fino alla definizione delle modalità di sanzionamento in caso di inadempimento.

La finalità del D.lgs. 196/2003 è quella di garantire che il trattamento dei dati personali venga eseguito nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il D.lgs. 196/2003 all'art. 4 lettera "a" disciplina il termine "trattamento" come qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Il trattamento, quindi, si concretizza in ogni tipo di operazione svolta su dati altrui, senza rilevare né il genere di operazione svolta, né il tipo di ausilio utilizzato per compierla. Tale genericità, voluta dal

[9] Da ricordare quindi tra le principali innovazioni alla legge 675/96, il decreto legislativo 28 dicembre 2001, n. 427, concernente disposizioni correttive ed integrative in materia di protezione dei dati personali. Questo provvedimento integra e modifica la normativa sul trattamento dei dati personali, meglio conosciuta come la legge 675/96.

[10] Distingue tre categorie di dati: comuni, sensibili e ipersensibili.

legislatore, permette un'applicazione estremamente ampia della disciplina, adattabile alle varie fattispecie che si potrebbero venire a creare nel corso del tempo.
Il D.lgs. 196/2003 non solo vale a dare un rigoroso inquadramento di sistema a tutta la disciplina della privacy, ma soprattutto introduce una molteplicità di profili innovativi, direttamente connessi al quadro comunitario e internazionale, sia completando il recepimento della direttiva 95/46/CE, sia ispirandosi ai più recenti elementi propulsivi rivolti a realizzare la nuova formula costitutiva dell'Unione Europea.

1.5 Il contesto europeo di riferimento

Le pronunce della Corte in tema di riservatezza fanno intendere una volontà di muoversi in due direzioni: da una parte, la vita privata collegata alla libertà, costituzionalmente garantita, di sviluppare la propria personalità (libertà di), dall'altra la vita privata declinata come il diritto alla protezione contro le altrui interferenze (libertà da). Una bidirezionalità resasi necessaria dal contesto socioeconomico caratterizzato da uno sviluppo tecnologico che ha appunto portato alla "società dell'informazione".
E' proprio sul trattamento dei dati personali che, nell'ultimo decennio, più intensa è stata l'attività legislativa (collegata all'evoluzione del diritto comunitario in materia).
La genesi della "*Privacy*" si può certamente rinvenire negli accordi di Schengen che vennero firmati il 14 giugno del 1985 nella città di Shengen, provincia Lussemburghese.
Gli stati che aderirono sin da subito furono solamente cinque: Belgio, Lussemburgo, Francia, Germania, Paesi Bassi, e solo in seconda istanza presero parte all'accordo altri stati europei, tra cui la stessa Italia il 27 novembre 1990.
Gli accordi prevedevano da un lato l'abolizione delle dogane nei paesi membri, dall'altro il rafforzamento dei controlli al di fuori dei confini dovuto ad una maggiore cooperazione delle forze di polizia tra i vari stati, nonché all'integrazione delle banche dati delle stesse forze armate.
Lo scopo iniziale del trattato di Shengen era quello di abbattere le barriere tra gli stati sottoscrittori al fine di ottenere un progresso economico, in seguito alla libera circolazione di persone e merci da uno stato membro ad un altro, senza la necessità di passare per una o più dogane, ottenendo di conseguenza un notevole abbassamento dei costi.
Con l'applicazione del trattato di Schengen, a seguito della libera circolazione di persone e merci, diventa naturale anche la circolazione a sua volta maggiormente "libera" di informazioni e dati personali, spesso sensibili.
Il rischio era quello di liberalizzare sì il settore economico all'interno dell'unione europea, ma senza porre attenzione alla circolazione di informazioni, naturalmente incrementata e fuori controllo in un contesto non regolamentato *ad hoc*.
La problematica in essere ha posto l'esigenza di provvedere quindi ad una maggiore disciplina per quanto concerne il trattamento di particolari informazioni, in particolare quelle sensibili.

Nasce così la direttiva del 46/95/CE, testo di riferimento a livello europeo in materia di dati personali, il cui ambito di applicazione fa riferimento a dati generati in modalità automatica (es. database informatico) o più generalmente a dati archiviati sotto varia forma sia tradizionale che digitale (es. archivi in formato cartaceo), e non fa riferimento alla vita domestica o personale del soggetto interessato.

CAPITOLO SECONDO

Il Garante e la Pubblica Amministrazione

2.1 Nascita dell'Autorità Garante

Dopo l'emanazione della legge sulla privacy, la 675/96, nacque l'esigenza di creare un organo collegiale imparziale e con una propria soggettività giuridica al fine di avere un ente che garantisse la supervisione della materia di protezione dei dati personali nel nostro paese.

L'autorità garante fu creata dal parlamento nel 1997 non solo con lo scopo di avere un organo che supervisionasse la legge, ma anche con l'obiettivo che rispondesse alle esigenze di chiarimenti della società in merito alla materia di protezione dei dati personali.

Uno dei compiti più difficili per il garante è quello di comunicare l'esattezza della normativa alla collettività. Per svolgere al meglio la comunicazione all'esterno questi si avvale di bollettini che raccolgono provvedimenti, risposte ai quesiti dei media e degli organi di stampa che si pongono come obiettivo la corretta divulgazione attraverso le proprie testate giornalistiche degli approfondimenti inviati dal garante settimanalmente.

Infine, per ottimizzare la promozione informativa, è stato realizzato il sito web del garante, anch'esso aggiornato periodicamente.

L'autorità garante ha sede in Roma, ove vengono svolte le riunioni, le quali possono essere tenute anche in videoconferenza.

Essendo un organo amministrativo indipendente, il Garante ha una propria soggettività giuridica ed esercita il suo potere di vigilanza in materia della privacy.

Il mandato dei membri del garante dura quattro anni. Decorso questo lasso di tempo il Parlamento provvede all'elezione di un nuovo organo collegiale.

Il presidente raffigura il Garante, e viene eletto dai componenti a scrutinio segreto con il voto di almeno tre componenti. Se tale maggioranza non è raggiunta dopo la terza votazione, è eletto presidente il componente che consegue il maggior numero di voti e, a parità di voti, il più anziano di età[11].

I membri del collegio non possono esercitare attività professionali o di consulenza, né essere amministratori di enti pubblici o privati, né ricoprire cariche elettive, al fine di garantire una totale indipendenza.

2.2 Compiti del Garante

Il Garante con l'entrata in vigore della 675/1996 ha dovuto fare fronte a molti interventi, soprattutto in situazioni in cui la normativa della *privacy* va ad impattare casi particolari che con il diffondersi delle tecnologie, cresciute in modo esponenziale, hanno dato origine a possibili vuoti normativi. Di conseguenza anche l'autorità garante ha dovuto evolversi per continuare a far sì che la normativa venisse rispettata.

Si pensi ad esempio alle segnalazioni, ai reclami, alle ispezioni e ai controlli, alle autorizzazioni generali ed individuali per il trattamento di dati sensibili, alla creazione del registro generale dei trattamento in cui sono archiviate le notifiche, all'organizzazione e al funzionamento dell'ufficio, alla predisposizione di un proprio codice etico, ai rapporti con i media, ai bollettini volti alla divulgazione degli aspetti trattati dall'autorità e altro.

I compiti del garante vengono definiti nel art. 154 del D.lgs. 196/2003.

Gli adempimenti principali che permettono al garante e ai terzi di conoscere se, perché e come una determinata azienda o ente gestisca dati sensibili sono: la notificazione all'autorità garante, l'informativa all'interessato, la raccolta dei consensi, la suddivisione dei compiti con l'attribuzione delle relative responsabilità all'interno delle organizzazione del titolare e l'adozione di determinate misure di sicurezza.

[11] www.garanteprivacy.it

La notificazione è una comunicazione ufficiale che il titolare del trattamento deve inviare per via telematica al Garante, con la quale gli si comunica l'esistenza di un'attività di raccolta e utilizzazione di dati personali e informazioni sul tipo di trattamento svolto.

Essa deve essere inviata al Garante qualora il titolare effettui il trattamento di: dati biometrici o genetici, quando il dato rileva la posizione geografica di persone od oggetti mediante mezzi di comunicazione elettronica, dati che rilevano la vita sessuale e lo stato di salute di un soggetto, come in caso di prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazioni di malattie mentali, infettive e diffusive, coma la sieropositività, il trapianto di organi e tessuti ed infine il monitoraggio della spesa sanitaria.

Occorre notificare anche i dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti.

E ancora dati sensibili registrati in banche dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie, dati registrati in apposite banche dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti e infine dati concernenti l'ubicazione di persone o oggetti mediante una rete di comunicazione elettronica.

Questo ultimo tipo di raccolta di dati, è ormai possibile grazie alle tecniche che consentono di individuare la localizzazione geografica degli utenti di telefonia mobile. Un altro esempio deriva dalla possibilità di rintracciare l'acquirente di un prodotto a cui sia stata applicata la cosiddetta "etichetta intelligente", ancora in fase di sperimentazione, che consentirebbe, attraverso un microchip applicato a un qualsiasi bene, la possibilità di verificare i movimenti dei singoli articoli in vendita.

Questo dispositivo comporterebbe anche dei rischi per la *privacy* delle persone, poiché tiene monitorato per ogni acquirente il tipo di acquisto nei casi in cui il microchip è stato inserito. Una forma simile di controllo si verifica abitualmente con i dati registrati per la "spesa automatica" e attraverso le "carte fedeltà".

Grazie a quest'ultime è possibile conoscere gli acquisti collegati alla carta e di collegarli quindi con l'anagrafe completa del possessore della carta. Con la "spesa automatica", progetto sviluppato da note catene della grande distribuzione, è anche possibile tracciare l'ordine con cui un utente compra un bene, informazione utile per finalità di marketing.

Tracciare gli acquisti di una persona aiuta a definire il profilo di essa e probabilmente a ricostruire informazioni sensibili che vanno anch'esse, quindi, trattate e tutelate.

Ai sensi dell'art.38, primo comma, D.lgs.196/2003, la notificazione deve essere presentata anche una sola volta, anteriormente all'inizio del trattamento, indipendentemente dalla durata sua durata e dalla numerosità delle operazioni e può riguardare una o più finalità correlate. Una nuova notificazione è necessaria soltanto

qualora vi sia cessazione del trattamento o se si assista ad una variazione di uno o più elementi, da indicare nella notificazione stessa.

L'informativa è la comunicazione con la quale il titolare del trattamento informa l'interessato del trattamento svolto, e può essere tipo orale o scritta. Il titolare deve illustrare all'interessato la finalità e modalità del trattamento dati, l'ambito di comunicazione e diffusione dei dati, eventuali conseguenze di un rifiuto del conferimento, eventuale trasferimento all'estero dei dati, i diritti dell'interessato, indicazioni del titolare, l'indicazione del Responsabile individuato o di quello designato per l'esercizio dei diritti dell'interessato, l'indicazione degli Incaricati che compiono le operazioni di trattamento.

L'informativa va resa al responsabile al momento della raccolta dei suoi dati.

Per raccolta di consensi sin intende che, non si può effettuare un trattamento dati senza il consenso del titolare, e deve essere esplicito, libero e documentato per iscritto. Con il consenso l'interessato esprime l'autorizzazione in senso generale al trattamento dei suoi dati. La mancanza del consenso comporta sanzioni penali e amministrative, ferma restando la responsabilità civile del Titolare in caso di accertamento del danno derivante da illecito trattamento.

L'art. 24 del decreto legislativo 196/2003 raccoglie i casi in cui non vi è bisogno di chiedere il consenso per il trattamento.

Il titolare può dare il proprio consenso sul trattamento discriminando alcune operazioni di trattamento, escludendone altre seppur facendo parte dello stesso trattamento. Ad esempio, il consenso può essere prestato solo per la registrazione dei dati, ma non per la loro elaborazione o per il loro raffronto con altri dati.

La tutela alla riservatezza non si delimita solo al rispetto dei principi di correttezza e liceità delle singole operazioni del trattamento eseguite dai differenti titolari, ma deve estendersi sino a comprendere sistemi tecnici, organizzativi, logistici che consentano una effettiva e concreta protezione della sfera privata dell'interessato.

Assume notevole importanza, nel complesso introdotto dalla normativa, la tutela dei dati personali non che la sicurezza delle operazioni di trattamento che deve essere garantita di pari passo con l'evoluzione tecnologica raggiunta nella consapevolezza che siamo in presenza di una sempre maggiore proliferazione dei rischi a cui i dati personali sono quotidianamente sottoposti. La crescita esponenziale di internet e l'evoluzione di mezzi tecnologici sofisticati, hanno fatto sì che la trasmissione dei dati possa avvenire senza alcuna limitazione territoriale mettendo a rischio la loro effettivamente sicura archiviazione.

I nuovi mezzi di comunicazione legati alla rete internet sono quindi molto rischiosi, in quanto permettono l'interferenza da parti di terzi in mancanza di precise procedure ed aggiornati criteri di sicurezza.

L'adozione di idonee misure di sicurezza è strettamente correlata con la riduzione dei costi, che il titolare dovrebbe sostenere al verificarsi dell'alterazione o della divulgazione di dati personali, spesso di natura sensibile. Deve, pertanto, svilupparsi una maggiore conoscenza della sicurezza ed una sensibilizzazione al trattamento attraverso la pianificazione di un budget di spesa dedicato agli aggiornamenti e alla configurazione di sistemi informatici idonei. L'adozione di aggiornate misure di sicurezza deve essere

garantita dal momento della pianificazione di un trattamento e sin dalla sua concreta esecuzione. Il legislatore italiano ha individuato alcune regole di base considerate minime e definite nel D. Lgs.196/2003.
Il Garante deve controllare che i trattamenti dei dati sensibili vengano effettuati nel rispetto della disciplina e in conformità alla notificazione anche in caso di cessazione dei trattamenti.
Deve esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o alle associazioni che li rappresentino.
Questa attività ha luogo in quanto il Garante riceve reclami da singoli privati, da associazioni di consumatori che avvisano il Garante della non osservanza della normativa.
Deve prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento lecito qualora vengano segnalati reclami. Deve vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco, ovvero emettere blocchi correttivi.
Segnalare a parlamento e governo l'opportunità di procedere con interventi normativi per fare si che i diritti di libertà, dignità, riservatezza, protezione dei dati vengano rispettati.
Deve inoltre esprimere pareri qualora vengano richiesti. Ma soprattutto deve diffondere la conoscenza tra l'utenza della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati.
Si occupa di denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle proprie funzioni. Tenere il registro dei trattamenti formato sulla base delle notificazioni e promuovere il codice di deontologia e buona condotta.
Annualmente il Garante è tenuto a predisporre una relazione sull'attività svolta e sullo stato di attuazione del presente codice, che viene trasmessa al parlamento e al governo entro il 30 Aprile dell'anno successivo a quello cui si riferisce.
Deve inoltre svolgere la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da regolamenti comunitari.
In particolare, il Garante deve aggiungere ai compiti appena espressi, il dovere di modifica, di ratifica e di esecuzione dei protocolli e degli accordi di adesione all'accordo di Schengen non che alla relativa convenzione di applicazione e alle successive modificazioni, di ratifica ed esecuzione della convenzione istitutiva dell'Ufficio europeo di polizia (*Europol*) e alle successive modificazioni, di ratifica ed esecuzione, della convenzione sull'uso dell'informatica nel settore doganale.
Deve inoltre attenersi al regolamento (Ce) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'"***Eurodac***" per il confronto delle impronte digitali e per l'efficace applicazione della convenzione di Dublino.
Il Garante coopera con altre autorità amministrative indipendenti nello svolgimento dei rispettivi compiti. A tale fine, il Garante può anche invitare rappresentanti di un'altra autorità a partecipare alle proprie riunioni, o essere invitato alle riunioni di altre autorità, prendendo parte alla discussione di argomenti di comune interesse ove può richiedere, altresì, la collaborazione di personale specializzato addetto.

Un aspetto molto importante dell'attività dell'autorità garante è il rilascio delle autorizzazioni per il trattamento dei dati sensibili e giudiziari, nonché al trasferimento dei dati all'estero. Il compito correlato al rilascio delle autorizzazioni consiste nel valutare se la richiesta fatta dal responsabile in merito a un trattamento dati sia idonea o meno. Le autorizzazioni possono essere di tipo individuali, rilasciate al singolo titolare, o di tipo collettivo, rilasciate dalle ***autorizzazioni collettive.***

Le autorizzazioni collettive nascono con la finalità di alleggerire la burocrazia e l'organizzazione delle attività per il garante.

Le autorizzazioni generali permettono ad un titolare di non richiedere il consenso per un determinato trattamento, sempre che il trattamento medesimo rispetti i limiti e le prescrizioni contenute nelle autorizzazioni collettive. Le richieste di autorizzazione individuali posso essere fatte tramite la modulistica messa a disposizione dal garante con gli stessi mezzi messi a disposizione per le notifiche.

La funzione del Garante si esplica attraverso interventi di carattere inibitorio, cautelare o sanzionatorio finalizzati alla risoluzione dei conflitti fra l'interessato ed il titolare del trattamento. Questa funzione può essere attivata d'ufficio o a seguito di una segnalazione o di un reclamo. Questi poteri sono perciò indirizzati alla prevenzione ed alla repressione di illeciti in materia e possono essere esercitati tanto nei confronti di un intero trattamento quanto in riferimento ad una sua parte soltanto.

L'art.157 del D.Lgs 196/2003 stabilisce che il Garante possa richiedere al titolare, al responsabile, all'interessato o anche a soggetti terzi di fornire informazioni e di esibire documenti. E' questa una prima modalità di verifica sulla corretta applicazione della legge sulla privacy, volta ad acquisire primi elementi di valutazione che possono essere sufficienti allo scopo di indurre il garante a procedere verso controlli più specifici e circostanziati, che si esplicano in accertamenti ed ispezioni, nonché ad accessi a banche dati.

Viceversa, è possibile che, a seguito di accertamenti, il garante possa richiedere l'esibizione di documentazione o il rilascio di altre informazioni.

L’accesso alle banche dati, le ispezioni e le verifiche possono essere eseguite informando il titolare o il responsabile o, se è assente o non nominato, anche gli incaricati del trattamento. Il personale d'Ufficio deve essere munito di documento di riconoscimento e può essere assistito da consulenti. Possono essere estratte copie di documenti, anche a campioni e su supporto informatico o per via telematica. Al termine delle operazioni di accertamenti sarà redatto un verbale riportante i risultati dell'ispezione e anche eventuali dichiarazioni dei presenti. Una volta terminato l'accertamento, il Garante rileva la violazione della normativa, e se sussistono elementi probatori del trattamento illecito e non conforme al codice, indica al responsabile o al titolare le misure modificative o integrative a correzione, e ne verifica l'adozione. Se l'accertamento è stato richiesto dall'interessato, il garante provvederà a comunicargli l'esito dell'accertamento.

Il codice etico del Garante nasce con il fine di dare un esempio a quei settori nei quali viene promossa la disciplina. L'obiettivo del codice etico è quello di definire una serie di linee guide di comportamento che i soggetti che compongono l'ufficio del garante devono eseguire nello svolgimento della loro attività. Questi

principi si concretizzano nei doveri di lealtà, di imparzialità, di diligenza e di operosità. Coloro che operano per l'Autorithy devono svolgere i propri compiti tenendo ben presente i doveri di indipendenza e di rispetto degli obblighi di riservatezza e segretezza delle informazioni conosciute nell'ambito delle proprie mansioni e, non ultimi, i principi di imparzialità e di trasparenza delle proprie mansioni e nelle attività di amministrative.

Devono essere mantenute la riservatezza assoluta nei confronti di tutte le informazioni acquisite nell'espletamento delle proprie mansioni ed anche successivamente alla cessazione del periodo di servizio presso l'ufficio. I dipendenti dell'Ufficio devono essere cordiali, efficienti e disponibili, onde manifestare il proprio impegno a favore della salvaguardia della privacy delle persone. Analogo deve essere il comportamento nei confronti dei colleghi e collaboratori e dipendenti dell'ufficio.

Per dovere di imparzialità si intende che non siano ammessi favoritismi, situazioni privilegiate e condizionamenti.

Nel codice etico è affrontato anche il tema del conflitto di interesse che potrebbe sorgere in riferimento ad attività precedenti svolte dal componente dell'Ufficio: il dipendente deve astenersi dal partecipare, per almeno due anni, dal trattare questioni che sono di competenza del Garante e che coinvolgono propri precedenti soci in affari o precedenti datori di lavoro. Alla base del codice etico stanno i principi di condotta che perseguono il fine di raggiungere la correttezza professionale, inibendo qualsiasi atteggiamento, azione o dichiarazione che rischi di sminuire il ruolo di giudice imparziale.

Questa specifica regola di condotta è evidenziata con particolare riferimento ai rapporti con gli organi di stampa.

Il codice etico, può, infine, essere aggiornato sulla base dell'esperienza acquisita nel corso del tempo, senza porre una scadenza sistematica ad una sua messa in discussione.

2.3 Privacy e Pubblica Amministrazione: una difficile convivenza

Nel riordinare la materia della tutela alla riservatezza, il nuovo codice ha adottato una struttura piuttosto complessa che crea numerosi problemi di interpretazione logica delle norme.

Si sovrappongono criteri soggettivi ed oggettivi - funzionali per l'individuazione delle singole regole applicabili, in un rincorrersi di regole generali ed eccezioni di difficile lettura, nulla di paragonabile, al caos linguistico della legge precedente.

Il rapporto tra privacy e pubblica amministrazione non è mai stato semplice e più in particolare, non lo è stato quello tra trasparenza nell'amministrazione e tutela e gestione dei dati personali in mano pubblica.

La pubblica amministrazione, come ogni altro soggetto, pubblico o privato, persona fisica o giuridica, ha bisogno della maggiore quantità di informazioni possibili per poter esercitare al meglio le proprie attività e svolgere in maniera più efficace le proprie funzioni. Per cui la gestione delle informazioni diventa espressione del principio costituzionale sancito nell'art. 97, e del suo rispetto. D'altra parte molte di queste informazioni riguardano i dati sensibili e a volte estremamente sensibili dell'individuo.

La Pubblica Amministrazione diventa pertanto "custode" di dati personali, ma nel momento stesso in cui essa cerca, ottiene e gestisce dati personali, mal sopporta i limiti fissati dalla normativa posta a tutela della riservatezza (o meglio dei dati personali, visto il solenne riconoscimento nell'art. 1 del Codice), in quanto il rispetto di tali regole rende ovviamente più difficile e meno spedita la sua azione.

La nuova disciplina dei dati personali, quando affronta le tematiche di questi rapporti tra privacy e pubblica amministrazione, deve considerare il ruolo della stessa, e in particolare gli interessi pubblici e privati, collettivi, diffusi e individuali, primari e secondari che devono essere ponderati dall'attività dell'amministrazione. Non si tratta di una cosa di facile realizzazione per una serie di motivi: la mole di dati, la rilevanza degli interessi ed il loro incrocio, le dinamiche amministrativistiche sottesi, la potenziale offensività dei comportamenti dei soggetti pubblici, la necessità di un connubio tra riservatezza e azione della pubblica amministrazione. La riservatezza, infatti, non indica più solo una posizione sostanzialmente passiva della persona, che si sostanzia nell'intolleranza di ingerenze esterne, ma è qualcosa di più. Grazie prima alla legge 675/96, ed ora, al decreto legislativo n. 196 del 2003 e, quindi, con la codificazione del diritto all'autodeterminazione informativa, ciascuno di noi può proteggere i propri dati personali, avendo ciascuno il diritto di proporsi agli altri negli esatti termini in cui vuole che ciò accada, decidendo in anticipo quali informazioni personali è disposto a dare agli altri soggetti.

Il diritto positivo ha ormai proposto una concezione dinamica del concetto di riservatezza e di identità personale: ed in questo consiste il grande mutamento.

Si delinea ora la nuova frontiera dei diritti fondamentali dell'individuo e del cittadino, rapportati all'operato della pubblica amministrazione.

In effetti, dobbiamo registrare un rapporto interattivo tra i due termini - del tema pubblica amministrazione - diritti del cittadino.

Tra queste due entità (la pubblica amministrazione e il complesso delle posizioni soggettive) intercorre una relazione di reciproca influenza, di modifica e di rinnovamento. Per poter naturalmente corrispondere alla nuova serie di diritti generati dalla normativa europea e dalla recente legislazione nazionale, la Pubblica Amministrazione modifica il proprio ruolo, il proprio comportamento, il proprio modo di agire, al punto che si sostituisce all'amministrazione monologante la nuova formula dell’amministrazione dialogante, che apre un dialogo pieno, aperto con i cittadini.

2.4 Il regime differenziato nel trattamento dei dati in ambito pubblico

La pubblica amministrazione si configura come l'articolata struttura attraverso la quale lo Stato persegue i propri fini istituzionali volti a tutelare e garantire interessi primari della collettività.

L'entrata in vigore della legge 675/96[12] ha sicuramente rappresentato un momento di forte cambiamento nel modo di trattare le informazioni personali da parte delle pubbliche amministrazioni: la necessità di fornire

[12] Sito web http://www.parlamento.it/parlam/leggi/deleghe/03196dl.htm

l'informativa, l'obbligo di trattare i dati solo per lo svolgimento delle funzioni istituzionali e la rigida disciplina per la comunicazione e la diffusione dei dati sono vincoli che fino a quel momento, non avevano condizionato l'attività delle amministrazioni.

Le novità che hanno maggiormente preoccupato le amministrazioni, in relazione al maggior rigore della disciplina prevista, sono state tuttavia quelle relative al trattamento dei dati cosiddetti "particolari", ovvero, i dati sensibili.

Essi costituiscono il fulcro della privacy dell'individuo.

Tali dati hanno, infatti, rappresentato la base per le gravi discriminazioni che la lunga storia del genere umano deve purtroppo annoverare: convinzioni religiose, idee politiche, origini razziali o etniche, particolari condizioni di salute o abitudini sessuali, sono sempre state utilizzate per identificare il "diverso" e, nella migliore delle ipotesi, per allontanarlo dalla società cosiddetta "normale". Proprio per tale ragione già la Convenzione sui diritti umani del 1950, prevedeva il divieto generale di trattare tali dati, divieto ribadito nella Convenzione n. 108 che, nell'art. 6, si occupa delle "categorie speciali di dati", e ancora la direttiva n. 95/45/CE disciplina i trattamenti riguardanti "categorie particolari di dati". Seguendo l'impostazione della precedente normativa il Codice detta all'art. 20 i «principi applicabili al trattamento dei dati sensibili», restringendo ulteriormente la potestà di trattamento della Pubblica Amministrazione relativamente alla categoria dei dati sensibili e giudiziari.

La norma riflette un rigore di base già presente nella legge 675/96 ed ora confermato dalla novella legislativa la quale sembra seguire tre linee giuda: nel trattare i dati sensibili occorre sempre una norma di rango legislativo ed espressa che a tanto autorizzi il soggetto pubblico; la norma, una volta individuata, deve esplicitare il rilevante interesse pubblico; la norma deve indicare in maniera dettagliata le operazioni ed i trattamenti eseguibili.

Il soggetto pubblico vi si deve attenere scrupolosamente, non è consentita alcuna interpretazione induttiva ed estensiva. La norma in commento si segnala per una forte esigenza protezionistica di interessi privatistico-individuali che potremmo definire a «tutela preventiva rafforzata». I dati sensibili ai sensi dell'art. 4, comma 1, lettera d), sono, « i dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale». Dovrebbe dunque esistere, per ogni soggetto pubblico che ha necessità di trattare dati sensibili, una «espressa disposizione di legge» che lo autorizzi ad operare e che indichi in modo altrettanto esplicito, tipi di dati sensibili trattabili, ì tipi di operazioni consentite e le rilevanti finalità conseguite.

In assenza di una legge dal contenuto siffatto, il trattamento dei dati sensibili risulterebbe precluso. Ma l'art. 20 si dichiara norma fondamentale allorché prescrive che, anche in presenza di una legge che «specifica la finalità dì rilevante interesse pubblico, ma non individui «i tipi di dati e di operazioni eseguibili», il trattamento non potrà essere omnibus, ma sarà circoscritto ai soli dati ed operazioni «identificati e resi

pubblici a cura dei soggetti» che lo effettuano e pur sempre nel rispetto di «specifiche finalità » perseguite case by case secondo i principi guida previsti dall'art. 22 del Codice.

In definitiva, alla presenza di questa situazione, il soggetto pubblico interessato, per proseguire nel trattamento dei dati sensibili, deve sopperire alla lacuna delle leggi attraverso l'approvazione interna e l'adozione di un atto regolamentare, che corrisponde e soddisfa condizioni prestabilite.

Inoltre la legge prende in considerazione l'ipotesi estrema che si realizza quando la legge di settore non solo non specifica i dati sensibili trattabili e le operazioni eseguibili ma neppure prevede in modo esplicito il trattamento dei dati sensibili che pertanto deve essere desunto in modo esplicito dalle finalità istituzionali del soggetto. In assenza di un'espressa disposizione di legge, il trattamento può essere chiesto al Garante, con un procedimento simile a quello previsto per i privati. Appare in tutta evidenza l'attenzione del legislatore per i dati sensibili a cui, come per i privati anche in ambito pubblico, dedica una serie di garanzie preventive per il trattamento che intanto sarà possibile in quanto strettamente necessario ad assolvere interessi pubblici rilevanti e previsti da norme di rango legislativo o su espressa autorizzazione del Garante.

L'art. 20, infine, si chiude con un implicito richiamo all'art. 11 del Codice ed in particolare alla lettera e) per la quale i dati personali debbano essere «esatti» e se necessario «aggiornati»; questa è un'ennesima espressione di quella «tutela procedimentale» che consente al soggetto pubblico di esprimere in ogni «fase» e «grado» del trattamento, un controllo diretto sulla regolarità del medesimo nonché sulla «esattezza» e «attualità» delle informazioni che lo riguardano.

La norma in esame, inoltre, non assegna alla singola amministrazione il potere di "decidere", con ampia discrezionalità, i dati trattabili, ma attribuisce il solo potere di "identificare" i dati e le operazioni. In questi termini per altro, la Pubblica Amministrazione, deve limitarsi a valutare quali dati e quali operazioni sono essenziali per il perseguimento delle finalità per le quali il trattamento è stato "autorizzato".

Simili considerazioni valgono per i dati giudiziari, art. 21, che sono accostati a quelli sensibili per le stesse ragioni riguardanti l'estrema delicatezza di contenuto di questo tipo di informazioni che giustifica un elevato grado di vincoli e condizioni posti a tutela della riservatezza dell'individuo. L'idea che traspare dalla norma, è quella che i dati giudiziari sono una vera e propria species del genus «dati sensibili».

2.5 I principi applicabili da parte della Pubblica Amministrazione

Una norma molto importante in materia di riservatezza nell'ambito pubblico è l'art. 22 del Codice che detta una sorta di “statuto procedimentale” per il trattamento dei dati sensibili e giudiziari effettuato da parte dei soggetti pubblici: a differenza degli artt. 20 e 21, che individuano i presupposti del trattamento, l'art. 22 disciplina proprio le modalità operative del medesimo. L'articolo in commento riproduce quasi integralmente i principi introdotti dalla legge 135/1999 in materia di dati sensibili e giudiziari da parte della Pubblica Amministrazione. La norma esordisce con una regola che esprime un dovere di cautela preventiva

obbligando i soggetti pubblici al trattamento dei dati sensibili e giudiziari con «modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e delle dignità dell'interessato»[13].

E' una previsione molto significativa perché "sacrifica" un'esigenza di tipo pubblicistico dinanzi a valori centrali dell'ordinamento, come la libertà e la dignità dell'interessato. In tale contesto si potrebbe sostenere che il soggetto pubblico, la Pubblica Amministrazione, viene obbligato a "responsabilizzarsi" proprio mediante la chiara esposizione dei motivi che giustificano il potere del trattamento. E ancora, l'interessato non è assistito in maniera statica durante il trattamento dei propri dati, poiché l'art. 22, al comma 5° richiamando espressamente altri articoli del Codice, garantisce il rispetto dei principi di pertinenza, proporzionalità e necessità del trattamento, obbligando il soggetto pubblico ad una verifica periodica dei requisiti per l'utilizzo dei dati[14]. Un'ulteriore cautela imposta al soggetto pubblico riguarda l'obbligo di monitoraggio dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

La seconda parte dell'art. 22, mira a garantire un grado di protezione aggiuntiva rispetto a quella preventiva della prima parte dell'articolo: una protezione aggiuntiva che si sostanzia nell'obbligo a carico dei soggetti pubblici di trattare i dati sensibili e giudiziari contenuti in elenchi, registri o banche dati elettroniche, con tecniche di cifratura o l'utilizzazione di codice di accesso che rendono il dato temporaneamente inintelligibile anche al soggetto autorizzato ad accedervi, di modo che la cognizione e la conoscenza di quei dati siano permessi soltanto se necessario[15].

In definitiva l'art. 22 si potrebbe definire come una sorta di *vademecum* per il trattamento dei dati sensibili e giudiziari in ambito pubblico.

2.6 Le forme di tutela

Nel caso in cui ci fosse qualcuno che ritenesse di aver subito un comportamento lesivo di quanto disciplinato dalla normativa del Codice, sono possibili due forme di tutela: una amministrativa e l'altra giurisdizionale.

Relativamente alla prima l'interessato può rivolgersi al Garante mediante tre atti:

- reclamo circostanziato, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali;
- segnalazione, se non è possibile presentare un reclamo circostanziato, al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima;
- ricorso, se intende far valere gli specifici diritti di cui all'articolo 7 (diritto di accesso ai dati personali ed altri diritti) del D. Lgs. n. 196/2003.

2.6.1 Tutela amministrativa

[13] Sito web http://www.parlamento.it
[14] In pratica, la Pubblica Amministrazione deve valutare con cadenza periodica i dati sensibili e giudiziari
[15] Bellocci-Magnanensi-Passaglia-Rispoli, op. cit.

2.6.1.1 Il reclamo

Il reclamo contiene un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonché gli estremi identificativi del titolare, del responsabile, ove conosciuto, e dell'istante. Il reclamo è sottoscritto dagli interessati, o da associazioni che li rappresentano ed è presentato al Garante senza particolari formalità. Il reclamo reca in allegato la documentazione utile ai fini della sua valutazione e l'eventuale procura, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica, telefax o telefono.

Il Garante può predisporre un modello per il reclamo da pubblicare nel Bollettino e di cui favorisce la disponibilità con strumenti elettronici.

Esaurita l'istruttoria preliminare, se il reclamo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della definizione del procedimento:

a) può invitare il titolare, anche in contraddittorio con l'interessato, ad effettuare il blocco del trattamento ritenuto illecito o non corretto spontaneamente;

b) prescrive al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti;

c) dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera b), oppure quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati;

d) può vietare in tutto o in parte il trattamento di dati relativi a singoli soggetti o a categorie di soggetti che si pone in contrasto con rilevanti interessi della collettività.

I provvedimenti richiamati sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana se i relativi destinatari non sono facilmente identificabili per il numero o per la complessità degli accertamenti.

I provvedimenti appena elencati possono essere adottati anche a seguito delle segnalazioni, da presentarsi nella circostanza in cui è impossibile avanzare reclamo circonstanziato, se è avviata un'istruttoria preliminare e anche prima della definizione del procedimento.

2.6.1.2 Il ricorso

Il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria. La presentazione del ricorso al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto.

Salvi i casi in cui il decorso del termine esporrebbe taluno a pregiudizio imminente ed irreparabile, il ricorso al Garante può essere proposto solo dopo che è stata avanzata richiesta sul medesimo oggetto al titolare o al responsabile, e sono decorsi i termini di quindici giorni dal suo ricevimento, ovvero è stato opposto alla richiesta un diniego anche parziale. Il riscontro alla richiesta da parte del titolare o del responsabile è fornito, come già anticipato, entro quindici giorni dal suo ricevimento. Inoltre, se entro il plurimenzionato termine di

quindici giorni, le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessità, ovvero ricorre altro giustificato motivo, il titolare o il responsabile ne danno comunicazione all'interessato. In tal caso, il termine per l'integrale riscontro è di trenta giorni dal ricevimento della richiesta medesima.

Il ricorso è proposto nei confronti del titolare e indica:

a) gli estremi identificativi del ricorrente, dell'eventuale procuratore speciale, del titolare e, ove conosciuto, del responsabile eventualmente designato per il riscontro all'interessato in caso di esercizio dei diritti di accesso o di latri diritti di cui all'articolo 7 del D. Lgs. n. 196/2003;

b) la data della richiesta presentata al titolare o al responsabile, oppure del pregiudizio imminente ed irreparabile che permette di prescindere dalla richiesta medesima;

c) gli elementi posti a fondamento della domanda;

d) il provvedimento richiesto al Garante;

e) il domicilio eletto ai fini del procedimento.

Il ricorso è sottoscritto dal ricorrente o dal procuratore speciale e reca in allegato:

a) la copia della richiesta rivolta al titolare o al responsabile;

b) l'eventuale procura;

c) la prova del versamento dei diritti di segreteria.

Al ricorso è unita, altresì, la documentazione utile ai fini della sua valutazione e l'indicazione di un recapito per l'invio di comunicazioni al ricorrente o al procuratore speciale mediante posta elettronica, telefax o telefono. Il ricorso è rivolto al Garante e la relativa sottoscrizione è autenticata. L'autenticazione non è richiesta se la sottoscrizione è apposta presso l'Ufficio del Garante o da un procuratore speciale iscritto all'albo degli avvocati al quale la procura è conferita ai sensi dell'articolo 83 del codice di procedura civile, ovvero con firma digitale in conformità alla normativa vigente. Il ricorso è validamente proposto solo se è trasmesso con plico raccomandato, oppure per via telematica osservando le modalità relative alla sottoscrizione con firma digitale e alla conferma del ricevimento legislativamente prescritte, ovvero presentato direttamente presso l'Ufficio del Garante[16].

Il ricorso è inammissibile:

a) se proviene da un soggetto non legittimato;

b) in caso di inosservanza delle disposizioni in materia di interpello preventivo o se per il medesimo oggetto e tra le stesse parti è stata già adita l'autorità giudiziaria;

c) se difetta di taluno degli elementi indicati relativamente alla presentazione dello stesso, salvo che sia regolarizzato dal ricorrente o dal procuratore speciale anche su invito dell'Ufficio del Garante, entro sette giorni dalla data della sua presentazione o della ricezione dell'invito. In tale caso, il ricorso si considera presentato al momento in cui il ricorso regolarizzato perviene all'Ufficio.

[16] www.garanteprivacy.it

Il Garante determina i casi in cui è possibile la regolarizzazione del ricorso.

Fuori dei casi in cui è dichiarato inammissibile o manifestamente infondato, il ricorso è comunicato al titolare entro tre giorni a cura dell'Ufficio del Garante, con invito ad esercitare entro dieci giorni dal suo ricevimento la facoltà di comunicare al ricorrente e all'Ufficio la propria eventuale adesione spontanea. L'invito è comunicato al titolare per il tramite del responsabile eventualmente designato per il riscontro all'interessato in caso di esercizio dei diritti di accesso o altri diritti cui all'articolo 7, ove indicato nel ricorso. In caso di adesione spontanea è dichiarato non luogo a provvedere. Se il ricorrente lo richiede, è determinato in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso, posti a carico della controparte o compensati per giusti motivi anche parzialmente.

Nel procedimento dinanzi al Garante il titolare, il responsabile e l'interessato hanno diritto di essere sentiti, personalmente o a mezzo di procuratore speciale, e hanno facoltà di presentare memorie o documenti. A tal fine l'invito è trasmesso anche al ricorrente e reca l'indicazione del termine entro il quale il titolare, il medesimo responsabile e l'interessato possono presentare memorie e documenti, nonché della data in cui tali soggetti possono essere sentiti in contraddittorio anche mediante idonea tecnica audiovisiva. Nel procedimento il ricorrente può precisare la domanda nei limiti di quanto chiesto con il ricorso o a seguito di eccezioni formulate dal titolare. Il Garante può disporre, anche d'ufficio, l'espletamento di una o più perizie. Il provvedimento che le dispone precisa il contenuto dell'incarico e il termine per la sua esecuzione, ed è comunicato alle parti le quali possono presenziare alle operazioni personalmente o tramite procuratori o consulenti designati. Il provvedimento dispone inoltre in ordine all'anticipazione delle spese della perizia. Nel procedimento, il titolare e il responsabile possono essere assistiti da un procuratore o da altra persona di fiducia. Se gli accertamenti risultano particolarmente complessi o vi è l'assenso delle parti il termine di sessanta giorni può essere prorogato per un periodo non superiore ad ulteriori quaranta giorni. Il decorso dei termini previsti è sospeso di diritto dal 1° agosto al 15 settembre di ciascun anno e riprende a decorrere dalla fine del periodo di sospensione. Se il decorso ha inizio durante tale periodo, l'inizio stesso è differito alla fine del periodo medesimo. La sospensione non opera nei casi in cui sussiste un pregiudizio imminente ed irreparabile e non preclude l'adozione dei provvedimenti quali il blocco, in via provvisoria, in tutto o in parte, di taluno dei dati, ovvero l'immediata sospensione di una o più operazioni del trattamento.

Se la particolarità del caso lo richiede, il Garante può disporre in via provvisoria il blocco in tutto o in parte di taluno dei dati, ovvero l'immediata sospensione di una o più operazioni del trattamento. Il provvedimento può essere adottato anche prima della comunicazione del ricorso e cessa di avere ogni effetto se non è adottata la decisione entro sessanta giorni. Il medesimo provvedimento è impugnabile unitamente a tale decisione. Assunte le necessarie informazioni il Garante, se ritiene fondato il ricorso, ordina al titolare, con decisione motivata, la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione. La mancata pronuncia sul ricorso, decorsi sessanta giorni dalla data di presentazione, equivale a rigetto. Se vi è stata previa richiesta di taluna delle parti, il provvedimento che definisce il procedimento determina in misura forfettaria l'ammontare delle

spese e dei diritti inerenti al ricorso, posti a carico, anche in parte, del soccombente o compensati anche parzialmente per giusti motivi.

Il provvedimento espresso, anche provvisorio, adottato dal Garante è comunicato alle parti entro dieci giorni presso il domicilio eletto o risultante dagli atti. Il provvedimento può essere comunicato alle parti anche mediante posta elettronica o telefax. Se sorgono difficoltà o contestazioni riguardo all'esecuzione del provvedimento, il Garante, sentite le parti ove richiesto, dispone le modalità di attuazione avvalendosi, se necessario, del personale dell'Ufficio o della collaborazione di altri organi dello Stato. In caso di mancata opposizione avverso il provvedimento che determina l'ammontare delle spese e dei diritti, o di suo rigetto, il provvedimento medesimo costituisce, per questa parte, titolo esecutivo ai sensi degli articoli 474 e 475 del codice di procedura civile.

Avverso il provvedimento espresso o il rigetto tacito, il titolare o l'interessato possono proporre opposizione con ricorso. L'opposizione non sospende l'esecuzione del provvedimento.

2.6.2 La tutela giurisdizionale

La normativa recita che tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni del presente codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione, sono attribuite all'autorità giudiziaria ordinaria.

L'azione si propone con ricorso depositato nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento. Il tribunale decide in ogni caso in composizione monocratica. Se è presentato avverso un provvedimento del Garante adottato a seguito di reclamo, il ricorso è proposto entro il termine di trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito. Se il ricorso è proposto oltre tale termine il giudice lo dichiara inammissibile con ordinanza ricorribile per cassazione. La proposizione del ricorso non sospende l'esecuzione del provvedimento del Garante. Se ricorrono gravi motivi il giudice, sentite le parti, può disporre diversamente in tutto o in parte con ordinanza impugnabile unitamente alla decisione che definisce il grado di giudizio. Quando sussiste pericolo imminente di un danno grave ed irreparabile il giudice può emanare i provvedimenti necessari con decreto motivato, fissando, con il medesimo provvedimento, l'udienza di comparizione delle parti entro un termine non superiore a quindici giorni. In tale udienza, con ordinanza, il giudice conferma, modifica o revoca i provvedimenti emanati con decreto. Il giudice fissa l'udienza di comparizione delle parti con decreto con il quale assegna al ricorrente il termine perentorio entro cui notificarlo alle altre parti e al Garante. Tra il giorno della notificazione e l'udienza di comparizione intercorrono non meno di trenta giorni.

Se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impedimento, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio. Nel corso del giudizio il giudice dispone, anche d'ufficio, omettendo ogni formalità non necessaria al contraddittorio, i mezzi di prova che ritiene necessari e può disporre la citazione di testimoni anche senza la formulazione di capitoli. Terminata l'istruttoria, il giudice invita le parti a

precisare le conclusioni ed a procedere, nella stessa udienza, alla discussione orale della causa, pronunciando subito dopo la sentenza mediante lettura del dispositivo.

Le motivazioni della sentenza sono depositate in cancelleria entro i successivi trenta giorni. Il giudice può anche redigere e leggere, unitamente al dispositivo, la motivazione della sentenza, che è subito dopo depositata in cancelleria. Se necessario, il giudice può concedere alle parti un termine non superiore a dieci giorni per il deposito di note difensive e rinviare la causa all'udienza immediatamente successiva alla scadenza del termine per la discussione e la pronuncia della sentenza. Con la sentenza il giudice, quando è necessario anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile, accoglie o rigetta la domanda, in tutto o in parte, prescrive le misure necessarie, dispone sul risarcimento del danno, ove richiesto, e pone a carico della parte soccombente le spese del procedimento. La sentenza non è appellabile, ma è ammesso il ricorso per cassazione.

CAPITOLO TERZO

La PA tra accesso e riservatezza

3.1 Premessa

Il flusso di informazioni legato alla vita di ciascun individuo appartiene ad un sistema di circolazione dei dati che coinvolge oramai tutti i settori della vita sociale.

L'affermazione di un diritto del singolo al controllo della circolazione delle informazioni personali, attraverso l'applicazione della legge 675 del 1996, ed ora sancito espressamente dal Codice della privacy, si è arricchita con la dimensione della riservatezza come bene della vita suscettibile e meritevole di tutela grazie all'introduzione di nuovi canoni di comportamento degli operatori. L'individuazione, selezione e regolamentazione di questi comportamenti ha richiesto e richiede un costante e attento lavoro di interpretazione da parte dell'Autorità Garante che ne cura l'integrazione nei diversi settori dell'ordinamento. Con questo si vuole ribadire come si vada intensificando la funzione dell'Autorità Garante, non limitata al controllo ed alla giurisdizione concorrente con le altre Autorità giudiziarie, bensì volta a dare attuazione nel nostro ordinamento all'art. 3 della Costituzione sotto il profilo della dignità personale e dell'uguaglianza delle persone.

La rapida evoluzione del concetto di dignità della persona, comporta un progressivo ampliamento del diritto alla privacy nell'ordinamento, che acquisisce nuovi codici comportamentali tipizzati. A ciascuno di essi corrisponde un diritto personale ed assoluto che vuole sganciarsi dalla paterna "riservatezza" ed acquisire una propria autonomia. La riservatezza, pertanto, è certo dinamica in relazione al sostanziale divenire del vivere sociale, inteso come volontà di essere esclusi o comunque non subire interferenze, ma lo è anche con riguardo al potere di controllo delle proprie informazioni quando sono collocate nel contesto di situazioni giuridiche rilevanti per l'ordinamento.

In primo luogo, emerge l'interesse del singolo a non essere vittima del controllo pubblico e di ogni forma che attraverso di esso comporti una stigmatizzazione sociale.

L'evidente e necessario coinvolgimento della Pubblica Amministrazione nella disciplina del trattamento dati va così di pari passo con un'altra disciplina: quella dell'accesso ai documenti amministrativi.

Pertanto la disciplina del trattamento dati ha trovato un terreno fertile alla propria applicazione nel processo di rinnovamento dell'amministrazione pubblica, passando attraverso la porta aperta alla partecipazione del singolo cittadino all'esercizio imparziale ed efficiente dell'azione pubblica. Il diritto alla privacy è sicuramente un qualcosa di più che un "interesse serio" e può trovare, percorrendo questa strada, un efficace strumento atto alla precostituzione dei mezzi di tutela relativi a situazioni giuridiche soggettive non tanto limpide in cui si perdono i confini della dimensione del diritto.

Nell'ottica rappresentata, l'art. 7 del Codice 196 del 2003, è lo strumento con il quale il singolo può esercitare il potere di controllo su quei dati personali inseriti nel flusso di informazioni gestito dalla Pubblica Amministrazione, svolgendo allo stesso tempo la funzione di partecipazione al procedimento, finalizzata alla correttezza del trattamento dei dati e dello stesso procedimento in generale.

In questa accezione l'accesso è il mezzo attraverso il quale è possibile interagire con la Pubblica Amministrazione in ragione della finalità che si intende realizzare. La riservatezza, al contrario, può costituire un limite al principio della trasparenza dell'azione amministrativa, laddove le finalità e gli interessi che le motivano risultino contrapposte.

Occorre, pertanto, operare un costante bilanciamento dei due istituti i quali non sempre operano nella stessa direzione.

3.2 Il concetto di trasparenza

Ancora prima dell'elaborazione della legge 241/90, la dottrina rinveniva nella trasparenza l'imminente principio permeante la c.d. "casa di vetro"[17] che la P.A. doveva incarnare; tant'è che, pur nell'originario testo dell'art. 1 della legge n. 241/90 il termine "trasparenza" non compare affatto tra i principi della disciplina generale del procedimento amministrativo, si ritiene lo stesso collante dei vari fattori qualificanti il procedimento medesimo (responsabile del procedimento, motivazione, istituti di partecipazione, ecc.)

La trasparenza infatti (inserita solo con la novella del 2005 nell'art. 1 della legge sul procedimento) trascende la mera osservanza formale degli istituti del procedimento amministrativo perché viene percepita quale valore finalistico dell'ordinamento, espressione di democrazia politica ed amministrativa nonché valore strumentale e funzionale alla conoscibilità dei processi decisionali.

Proprio tale approccio finalistico consacra il rinnovato contesto relazionale tra amministrazione pubblica e cittadino ed il passaggio dal concetto di amministrazione-autorità a quello di amministrazione-servizio, dal concetto di amministrazione burocratica al concetto di amministrazione partecipata.

Il volano del cambiamento è da rinvenirsi pertanto nel contenuto che si intende attribuire al valore della trasparenza, ribaltando la tradizionale visione della amministrazione trincerata dietro il manto dell'impermeabilità fino a diventar regola generale la conoscibilità e l'intellegibilità dell'operato dei pubblici poteri.

Come tutti i valori anche per la trasparenza si corre il rischio di sfumare in un concetto assolutamente atecnico. Per scongiurare ciò deve intendersi in contrapposizione a tutto quello che si intende occultare per favorire interessi personali o di gruppo, configurandosi al contrario quale esigenza di chiarezza, di comprensibilità e di non equivocità di una organizzazione e del suo agire anche al fine di garantire il buon andamento dell'azione amministrativa. In tale prospettiva, la trasparenza è il viatico della chiarezza e della comprensibilità dell'azione amministrativa.

Alla luce di tal riflessione, si comprende come la trasparenza non possa esser confusa con la pubblicità o con l'accesso agli atti amministrativi rappresentando rispetto a questi ultimi un quid pluris che impone alla pubblica amministrazione un obbligo alla comprensibile esplicitazione del potere di cui è depositaria[18].

[17] www.commissioneaccesso.it, citazione di Filippo Turati

[18] Piazza, L., *Nuova trasparenza per la pubblica amministrazione*, www.diritto.it

La pubblicità è, infatti, una situazione prevalentemente "statica" afferendo al mero stato di fatto dell'atto, dell'organizzazione o del procedimento, lì dove la trasparenza attiene ad una dinamica relazionale, alla "intellegibilità" dei comportamenti amministrativi e delle scelte sottese.

Così è da definirsi sicuramente pubblico ma di certo non improntato ai criteri di trasparenza, un atto puntualmente pubblicato nell'albo o sul sito internet dell'amministrazione ma in periodo festivo ovvero occultato, ovvero non intuitivamente individuabile sul sito di riferimento, ovvero formalmente accessibile ma non comprensibile.

La trasparenza dunque si distingue dal diritto di accesso, pur rappresentando quest'ultimo uno dei principali strumenti di verifica dell'effettivo perseguimento del complesso dei valori che la trasparenza è volta a soddisfare. Infatti, la trasparenza è un fattore più ampio del mero accesso, atteso che può essere formalmente soddisfatto il diritto di accesso con l'ostensione di un atto amministrativo ma non essere garantita la trasparenza dell'azione amministrativa ove l'atto sia sostanzialmente incomprensibile nel suo contenuto.

Per converso, l'individuazione da parte delle amministrazioni pubbliche di categorie di atti sottratti al diritto di accesso può non essere in contrasto con la trasparenza ove si ritenga, nel contemperamento degli interessi sottesi, prevalente l'esigenza alla riservatezza. La problematicità del bilanciamento di tali valori viene percepita tanto nelle principali produzioni normative straniere e nazionali.

Infine, la necessità della comprensibilità dell'azione amministrativa appare coerente con una diffusa etica di sicurezza giuridica che, in uno Stato di diritto non può non informare i rapporti cittadino-amministrazione. Infatti, un'azione amministrativa "equivoca" o "irrazionale" rischia di disorientare i cittadini sui comportamenti da tenersi. Non a caso la Corte Costituzionale ha riconosciuto "l'affidamento del cittadino nella sicurezza giuridica" un elemento fondamentale dello stato di diritto. In tale contesto assume rilevanza particolare il D.Lgs. n. 150/2009 che all'art. 3 (la trasparenza dei risultati delle amministrazioni e delle risorse impegnate per il loro perseguimento) pone la stessa tra i principi volti all'ottimizzazione della produttività del lavoro pubblico, ed all'art. 11, stabilendo un collegamento tra performance e trasparenza, la definisce "accessibilità totale" riferita ad ogni informazione afferente l'aspetto dell'organizzazione, introducendo, per la prima volta, accanto al concetto di trasparenza, il valore dell'integrità, quale fattore culturale da sviluppare attraverso la programmazione e l'aggiornamento dei relativi piani triennali.

La configurazione della trasparenza quale accessibilità totale apre la stura al controllo sociale diffuso da parte della collettività sull'operato delle amministrazioni ponendosi quindi quale strumento finalizzato alla prevenzione di fenomeni di corruzione e in generale di *maladministration*. Tutto ciò segna la definitiva linea di demarcazione tra diritto di accesso e richiesta di trasparenza atteso che il primo resta spiazzato ove i dati siano necessariamente pubblici ed accessibili, pertanto, alla intera collettività al di fuori dell'ambito procedimentale in senso stretto.

Ne consegue che la migliore organizzazione amministrativa nella direzione della trasparenza sarà quella che si vedrà rivolgere limitate domande di accesso. Inevitabile, quindi, l'accelerazione ulteriore dei processi di riforma nelle amministrazioni pubbliche nella direzione dell'open government e delle problematiche

dell'open data. Sarà, pertanto, opportuno procedere alla individuazione dei dati rilevanti da pubblicare attraverso lo sviluppo di una politica di ascolto del cittadino quale fruitore finale del servizio.

3.3 L'accesso

Come detto nel paragrafo precedente all'interno del principio di trasparenza dell'attività amministrativa trova linfa vitale il fondamento giuridico del diritto di accesso. Il diritto di accesso ha avuto una lunga evoluzione normativa ma è stato introdotto quale principio generale del procedimento amministrativo all'interno della 241/90. Prima di tale data infatti il diritto di accesso agli atti era stato previsto solo in determinate ipotesi normative e solo limitatamente ad alcuni settori: prima della succitata 241/90 occorre ricordare le leggi n. 816/1985 e 142/90 in materia di accesso agli enti locali, e la legge n. 349/1986 in materia ambientale.

In cosa consista il diritto d'accesso ed in quali forme si estrinsechi lo si evince dalla lettera dell'art. 25 co. 1 della 241/90 secondo il quale "il diritto di accesso si esercita mediante esame ed estrazione di copia dei documenti amministrativi, nei modi e con i limiti indicati dalla presente legge".

La natura giuridica della situazione soggettiva facente capo al soggetto titolare del diritto di accesso viene qualificata come "diritto"[19].

Secondo parte della giurisprudenza non si tratterebbe di un diritto soggettivo in quanto tale diritto sarebbe da considerarsi limitato e sottoposto a discrezionalità, pertanto tale situazione potrebbe essere individuata solo come interesse legittimo, seppur particolarmente qualificato. Secondo un'altra branca della giurisprudenza il diritto di accesso dovrebbe essere considerato come diritto soggettivo all'informazione.

La legge 15/2005 innovando profondamente la 241/90 ha dettato una disciplina più organica e completa in materia di accesso ai documenti, disciplinato dal capo V agli artt. 22 e seguenti. Proprio l'art. 22 riconosce a chiunque vi abbia interesse la tutela di situazioni giuridicamente rilevanti il diritto di accesso ai documenti amministrativi precisando che è considerato documento amministrativo ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni o comunque utilizzati ai fini dell'attività amministrativa.

E' pertanto una definizione di documento amministrativo molto ampia e comprende tutto ciò che l'amministrazione conserva nei suoi archivi, riferendosi anche ad "atti interni" (esempio pareri), con ciò intendendosi non solo i documenti interni dell'amministrazione ma anche gli atti endoprocedimentali cioè gli atti che non hanno effetti immediato verso il privato ma costituiscono gli antecedenti del provvedimento finale (esempio pareri tecnici e nulla osta).

Inoltre il nuovo art. 22 dopo aver puntualizzato (lett. A) che il diritto di accesso è il diritto degli interessati di prendere visione ed estrarre copia dei documenti, alla lett. B indica come soggetti interessati, ossia i possibili titolari del diritto di accesso, "tutti i soggetti privati, compresi quelli portatori di interesse pubblici o diffusi,

[19] Zerman, P.M., *La trasparenza della p.a. tra accesso e privacy nella recente giurisprudenza del Consiglio di Stato*, www.giustizia-amministrativa.it

che abbiano un interesse diretto, concreto, attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso".

In particolare l'interesse deve essere:

- attuale, l'attualità viene valutata in base al momento in cui si fa richiesta di accesso ad un determinato documento;
- diretto, ossia personale, cioè deve appartenere alla sfera dell'interessato (e non ad altri soggetti, come ad esempio alle associazioni sindacali che spesso pretendono di agire facendo valere diritti dei singoli);
- concreto, cioè presuppone un collegamento tra il soggetto ed un bene della vita coinvolto dall'atto o documento;
- serio, ossia meritevole e non fatto valere al solo scopo di recare molestia o nocumento;
- adeguatamente motivato, con riferimento alle ragioni che vanno esposte nella domanda di accesso.

3.3.1 L'accesso civico

Il concetto illustrato di trasparenza si perfeziona a seguito dell'introduzione nel nostro panorama giuridico della figura dell'accesso civico, per effetto del D.Lgs. 14 marzo 2013, n. 33 che estende il campo di applicazione della normativa sul diritto di accesso.

La portata innovativa di tale istituto viene compresa se preliminarmente si tiene conto della circostanza che il decreto legislativo citato non è solo di riordino della tipologia degli obblighi di pubblicazione (incarichi esterni, beni e contratti pubblici, servizi sanitari…) che gravano sulle pubbliche amministrazioni, bensì ridefinisce la trasparenza "quale strumento al servizio dell'interesse alla conoscibilità degli elementi rilevanti ai fini di un controllo diffuso sull'operato delle amministrazioni". Ciò senz'altro nel solco delineato dalla legge 241/90 e successivamente dal decreto legislativo 150/09 (la trasparenza come accessibilità totale e ispiratrice unitamente ai criteri di economicità, efficacia e pubblicità dell'attività amministrativa), per giungere all'elaborazione di tre aspetti particolari dell'attuale accezione della trasparenza: la trasparenza come diritto, come obiettivo e infine come strumento di gestione della cosa pubblica e nella realizzazione dei servizi pubblici.

Infatti secondo quanto indicato dall'art. 5 del decreto citato in premessa, l'obbligo che dal medesimo è posto a carico delle pubbliche amministrazioni di pubblicazione di documenti, informazioni o dati, vede il diritto di chiunque di richiederne la pubblicazione se omessa. Ciò rappresenta la comunicazione all'esterno delle informazioni che devono pubblicarsi anche al di là del campo di applicazione dello stesso decreto, e altresì l'ampliamento dei confini oggettivi e soggettivi del diritto d'accesso. La domanda di accesso civico non è infatti condizionata né dall'obbligo della motivazione né dalla posizione soggettiva del richiedente. Mentre infatti il diritto di accesso è strumentale alla tutela di interessi specifici ed ha ad oggetto atti e documenti individuati, l'accesso civico sembrerebbe affiancarsi all'azione popolare e porsi come mezzo di verifica diffusa dell'attività amministrativa, da parte del cittadino. Potremmo parlare di "engagement", nel senso di impegno, di promessa e del dedicarsi agli interlocutori da parte dell'amministrazione e si potrebbe ancora

giungere ad ipotizzare una nuova forma di controllo “pubblico” accanto a quelle già previste dal sistema attuale dei controlli amministrativi e politici. Se infatti si pensa all’inciso di cui al comma 6 dell’articolo citato: “la richiesta di accesso civico comporta da parte del Responsabile della trasparenza, l’obbligo di segnalazione di cui all’art. 43, comma 5” ci si rende conto che poiché la segnalazione va resa anche al vertice politico ai sensi di tale comma, l’intera disciplina è finalizzata a dare effettività ai flussi dell’informazione pubblica, non solo a fini conoscitivi ma anche e soprattutto a fini di programmazione, di prevenzione e di controllo sociale.

Tale assunto è ancor più pregnante se si considera che la nomenclatura della legge anticorruzione pone in stretto contatto gli obblighi di pubblicità e la lotta alla corruzione: la funzione pubblica è infatti depositaria della fiducia pubblica. In tale ottica dunque, accanto alla predisposizione obbligatoria del Programma triennale per la trasparenza e l’integrità, è disciplinato l’istituto dell’accesso civico. Va tenuto presente che la richiesta di accesso civico va presentata al responsabile della trasparenza dell’amministrazione obbligata alla pubblicazione. Essa riveste inoltre il carattere della gratuità. Parrebbe dunque che si voglia incentivare il ricorso da parte dei cittadini a tale nuovo strumento, diffondendo sempre più tra i medesimi la cultura della trasparenza. Sicuramente è poi uno stimolo preventivo alle pubblicazioni, considerato che, ove le stesse non avvengono: 1. Si profila una delle ipotesi di responsabilità dirigenziale anche per danno all’immagine all’amministrazione; 2. Nei casi di ritardo o mancata risposta, il ricorrente ha la facoltà di rivolgersi al titolare del potere sostitutivo di cui all’art. 2, comma 9 bis della legge 241/90. La disciplina esaminata comporta inoltre per le pubbliche amministrazioni la necessità, ora imprescindibile, dell’adozione del sito web, in quanto successivamente alla richiesta di accesso civico e, nei trenta giorni successivi, occorre procedere alla pubblicazione in esso del documento o dell’informazione. Ciò conferma l’attuale riconoscimento delle potenzialità del web (in ciò la distinzione ulteriore con la disciplina del diritto di accesso in caso di accettazione della richiesta relativa) di pari passo alla necessità impellente ed al tempo stesso oggi costante, di contenere i dispendi della res publica. Si osserva però da parte della dottrina che “se già la trasparenza sancita dalla legge 241 aveva messo a dura prova le amministrazioni responsabili di aver impiegato troppo tempo per attrezzarsi, quella del decreto 33 potrebbe rivelarsi persino più impegnativa, arrivando a scontrarsi con la scelta (compiuta dalla legge delega 190) di ipotizzare che tutto possa concretarsi a risorse invariate”. In tal senso dunque l’accesso civico potrebbe rappresentare uno step significativo del processo citato in premessa di riorganizzazione della pubblica amministrazione in quanto il controllo che ne deriva e che è stato ora illustrato, induce l’amministrazione a comportamenti legittimi (in tal senso anche la recentissima adozione del nuovo codice di comportamento in vigore in questi giorni), rendendola finalmente “utile allo sviluppo sociale ed economico, con la conseguenza di limitare i tentativi ricorrenti di privatizzare e/o sopprimere enti amministrativi perché insufficienti”.

3.4 I "principi" generali in materia di procedimento amministrativo

Gli artt. 1, 2 e 3, contenuti nel Capo I della L. 7 agosto 1990, n. 241, dettano i principi generali in materia di procedimento amministrativo , a cui tutte le pubbliche amministrazioni devono attenersi, anche mediante adeguamento dei propri regolamenti. L'art 1, 1° comma, riafferma in termini assolutamente chiari, la subordinazione dell'attività amministrativa al principio di legalità, stabilendo che essa persegue esclusivamente i "fini determinati dalla legge". Ciò significa che l'attività amministrativa è costantemente vincolata in modo rigoroso al perseguimento dell' interesse pubblico determinato dal legislatore, non potendo essere "piegata" ad altri scopi non enunciati nei modi e nelle forme prescritte. Ne consegue, pertanto, il principio costituzionale dell' imparzialità dell' Amministrazione 13.

Lo stesso comma stabilisce, inoltre, che l'attività amministrativa "è retta da criteri di economicità, di efficacia, di pubblicità e di trasparenza".

Con la previsione del criterio di economicità/efficacia viene imposto alla P.A, la realizzazione del massimo risultato, quantitativo e qualitativo, in relazione ai mezzi a sua disposizione, e quindi il conseguimento degli obiettivi previsti con il minor dispendio di risorse e strumenti.

È bene puntualizzare che per "mezzi" devono intendersi non solo quelli di natura strettamente economica ma anche quelli di carattere procedurale; il legislatore ha così imposto di conformare l'azione amministrativa al criterio della massima effettiva economicità. È in questo contesto che si colloca il principio espresso dal 2 comma dell'art. 1, secondo cui "la Pubblica Amministrazione non può aggravare il procedimento, se non per straordinarie e motivate esigenze imposte dallo svolgimento dell'istruttoria".

Il principio di pubblicità si sviluppa e si completa nel principio di trasparenza dell'azione amministrativa; questi due principi assicurano la necessaria visibilità dell'azione amministrativa facendo conoscere ai cittadini, in modo semplice e completo, i contenuti e ìe forme di esercizio dell'attività amministrativa di modo che i cittadini stessi possano essere messi in grado di poter valutare l'attività amministrativa ed i risultati conseguiti.

Al criterio di pubblicità-trasparenza quindi, sono da ricondurre l'obbligo di rendere noti i termini e le unità organizzative responsabili del procedimento e di ogni altro adempimento, nonché l'organo responsabile dell'adozione del provvedimento finale, l'obbligo di motivazione del provvedimento amministrativo, nonché le procedure idonee a consentire l'accesso ai documenti amministrativi, tranne nei casi previsti dalla legge.

Inoltre l'Amministrazione per assicurare il principio di trasparenza è tenuta a provvedere alla pubblicazione di direttive, programmi, istruzioni, circolari, atti interpretativi di norme giuridiche o che dettano disposizioni per la loro applicazione.

Il termine accesso viene quindi comunemente usato come sinonimo di trasparenza e pubblicità, ma il principio di trasparenza si concretizza anche attraverso una serie di strumenti operativi introdotti e disciplinati dalla L. 241/90, tra i quali si annoverano:

a. l'obbligo di concludere il procedimento in modo esplicito entro un certo termine. L'art. 2, 1 comma recita infatti che "ove il procedimento consegua obbligatoriamente ad una istanza, ovvero debba essere iniziato d'ufficio, la pubblica amministrazione ha il dovere di concluderlo mediante l'adozione di un provvedimento

espresso". Si deve ritenere che il comportamento "inerte" della Pubblica Amministrazione, oltre a costituire, eventuale, fonte di responsabilità per i dipendenti cui è imputabile l'omissione, se da un lato consente all'interessato di promuovere le azioni amministrative e giurisdizionali volte ad accertare l'illegittimità del silenzio-inadempimento non preclude all'Amministrazione stessa, anche se sono ormai decorsi i termini previsti, di adottare un provvedimento espresso (sia esso di accoglimento o di diniego dell'istanza). La scadenza dei termini massimi previsti non esonera l'Amministrazione dall'obbligo di provvedere con ogni sollecitudine ed il responsabile del procedimento è esente da responsabilità personali solo ove esponga le ragioni del ritardo entro trenta giorni dal ricevimento della richiesta; tali giustificazioni, inoltre, non devono essere meramente dilatorie, con motivazioni stereotipe, generiche o pretestuose al fine di non incorrere nelle responsabilità previste dall'art. 328 c.p.

b. L'obbligo di motivazione del provvedimento amministrativo. La terza ed ultima disposizione riguardante i principi generali dell'attività amministrativa (art. 3 della legge n. 241 del 1990) stabilisce l'obbligo della motivazione per "ogni provvedimento amministrativo", con esclusione degli atti generali o a contenuto generale; la stessa norma fissa il contenuto minimo della motivazione. Non sembra superfluo rammentare, altresì, che sempre ai sensi dell'art. 3, ultimo comma, ogni atto notificato al destinatario deve contenere l'indicazione del termine e dell'autorità cui è possibile ricorrere.

c. La previsione di un responsabile del procedimento.

3.5 Il responsabile del procedimento amministrativo e l'attività di partecipazione al procedimento amministrativo

Mentre le disposizioni dei primi tre articoli del Capo I hanno valenza di "principi", gli articoli 4 - 6 del Capo II prevedono l'individuazione di un responsabile del procedimento e gli artt. 7 - 13 del Capo III individuano le modalità di intervento e di partecipazione al procedimento amministrativo.

In riferimento al Capo II, la normativa in argomento mira a consentire una più semplice e lineare organizzazione degli iter procedimentali e, al tempo stesso, a prevenire e reprimere comportamenti intenzionalmente o colposamente omissivi dei pubblici dipendenti.

In tale ambito assumono particolare rilevanza le figure del "responsabile del procedimento" e, nel caso in cui non coincidano, dell' "organo responsabile dell'adozione del provvedimento finale". Con l'individuazione, in concreto, dei soggetti (persone fisiche) abilitati a gestire e finalizzare l'attività amministrativa con le connesse responsabilità. La P.A. abbandona ogni idea di impersonalità e di anonimato dei suoi organi.

Il potere di assegnazione dei compiti di responsabilità dei singoli procedimenti, così come stabilisce l'art. 5, comma 1, spetta al dirigente dell' unità organizzativa, intendendosi per unità organizzativa responsabile del procedimento "la divisione o l'ufficio, centrale o periferico, o la sua articolazione(...)" - La prassi vuole che la persona preposta all'unità organizzativa sia anche il responsabile del procedimento prescindendo quindi e dalla titolarità dell'ufficio e dalla qualifica dirigenziale (l'accezione di "dirigente" contenuta nel primo comma della legge n. 241 del 1990 è da intendersi non perché in possesso della relativa qualifica, ma in

quanto "preposto" all'unità organizzativa). Il "dirigente" ha l'onere di individuare, in relazione a ciascun procedimento, la persona fisica del responsabile (se stesso o altro dipendente); nel caso in cui il responsabile dell'unità organizzativa abbia attribuito ad altri la cura di uno o più procedimenti, appaiono applicabili i principi giuridici che regolano l'istituto della delega.

I principali obblighi che la legge 7 agosto 1990 n. 241 attribuisce agli uffici ed, in particolare, al "responsabile del procedimento" sono:

a) curare la comunicazione con i destinatari degli effetti del provvedimento onde assicurarsi che gli stessi siano stati correttamente informati (art. 6);

b) comunicare l'avvio del procedimento ai soggetti nei cui confronti il provvedimento è destinato a svolgere i suoi effetti e a quelli ai quali il provvedimento stesso possa causare un pregiudizio. È bene chiarire che la comunicazione deve essere personale salvo il caso di esigenze di celerità o di eccessivo numero dei destinatari, per cui è possibile ricorrere a comunicazione mediante pubblicazione nel Bollettino Ufficiale del Ministero delle finanze, negli albi dell'amministrazione o con altre idonee forme (art 7, comma 1);

c) all'interno della comunicazione di avvio del procedimento devono essere indicati l'Amministrazione competente, l'oggetto del procedimento, l'ufficio ed il responsabile del procedimento, la data entro la quale deve concludersi il procedimento e i rimedi esperibili in caso di inerzia dell'amministrazione, l'ufficio in cui è possibile prendere visione degli atti, nonché il responsabile dell'adozione del provvedimento finale se diverso dall'organo indicato nel regolamento di attuazione del Ministero delle finanze, la data di presentazione dell'istanza ad iniziativa di parte (art. 8). Il responsabile del procedimento, relativamente ai procedimenti di competenza di organi dell'Amministrazione Finanziaria, deve comunicare entro 60 giorni all'interessato se la domanda risulti essere irregolare o incompleta, indicandone le relative cause (art. 3, comma 4, del regolamento) 17 e se non ritiene deve comunicare agli interessati la decisione di attendere il suddetto parere, per un periodo che comunque non può superare i 180 giorni (art. 7, comma 1, regolamento). Inoltre gli interessati devono essere informati della determinazione del Ministro di promuovere, nei casi di particolare rilevanza, l'intervento consultivo facoltativo del Consiglio di Stato, indicando contestualmente le ragioni di tale scelta nella stessa comunicazione (art 8, comma 1, regolamento). Infine, gli uffici devono consentire a chiunque vi abbia interesse di consultare gli appositi elenchi da cui risultino le unità organizzative responsabili dei procedimenti (art 13, comma 2, regolamento) e devono rendere note mediante pubblicazione o altre idonee fonti di pubblicità, le modalità per prendere visione degli atti dei procedimenti, ove ciò sia consentito (art. 5, comma 1, regolamento).

Qualunque soggetto, recita l'art. 9, portatore di interessi pubblici o privati, o di interessi diffusi costituiti in associazioni o comitati, cui possa derivare un pregiudizio dal provvedimento, ha facoltà di intervenire nel procedimento (art. 9) ed ha contestualmente il diritto di prendere visione degli atti e di presentare memorie scritte e documenti che l'amministrazione ha l'obbligo di valutare (art. 10). Si delinea chiaramente quella che è la finalità della L. 241/90 e cioè la tutela della posizione qualificata del pubblico cittadino che si concretizza nel diritto di accesso.

CAPITOLO QUARTO

Il panorama internazionale

4.1 Premessa: il modello europeo

In ambito europeo, la privacy è considerata un diritto fondamentale dell'individuo. Il suo primo riconoscimento avvenne con la "Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali" (CEDU) del 1950, il cui articolo 8 recita: "Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza". In questa sua prima formulazione, in linea con l'accezione adottata oltreoceano, il diritto alla privacy in Europa tendeva

sostanzialmente a coincidere con il diritto alla non intrusione nelle faccende di natura privata e familiare. La privacy come un vero e proprio diritto della persona al controllo dei propri dati personali ha trovato specifico riconoscimento in ambito europeo con la Convenzione n. 108 (la cosiddetta "Convenzione di Strasburgo" del 1981), riguardante la protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale[20].

In tale Convenzione per la prima volta in ambito europeo vengono stabiliti i principi per trattamento automatizzato dei dati personali (es. i principi di finalità, pertinenza e non eccedenza) e viene introdotta la definizione di dati personali, individuando in particolare i dati sensibili. Inoltre, viene garantita la possibilità di accesso degli individui alle informazioni che li riguardano direttamente.

La privacy è oggi consacrata nell'ambito della Carta dei Diritti Fondamentali dell'UE del dicembre 2000 (recepita poi nella parte iniziale del Trattato di Costituzione Europea, il cosiddetto Trattato di Lisbona in vigore dal 1° dicembre 2009), nonché nel Trattato sul Funzionamento dell'UE. In particolare la Carta riconosce i due seguenti distinti e complementari diritti fondamentali:

- *rispetto della vita privata e della vita familiare*: ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni (art. 7);
- *protezione dei dati di carattere personale*: ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano (art. 8).

Sulla scia della Convenzione di Strasburgo del 1981, nell'ambito della Comunità Europea viene introdotta una vera e propria disciplina organica sulla privacy attraverso la Direttiva 95/46/CE, (la cosiddetta "Data Protection Directive" o anche "Direttiva madre"), disciplina che è stata successivamente completata, per il settore delle comunicazioni elettroniche, dalle norme della Direttiva 2002/58/CE (cosiddetta "E-Privacy") e della Direttiva 2006/24/CE (quest'ultima relativa al trattamento dei dati di traffico per indagine, accertamento e perseguimento di gravi reati).

Il quadro normativo europeo è stato ovviamente concepito sul principio che la privacy è un diritto fondamentale dell'individuo, il quale va tutelato in quanto tale. Tutti i cittadini europei devono godere di un livello equivalente di protezione dei propri dati personali e, pertanto, le norme sono applicabili a tutti i settori industriali nel trattamento dei dati personali. Inoltre, alcuni settori sono soggetti ad ulteriori specifiche e molto spesso più stringenti norme, come quello delle comunicazioni elettroniche.

L'ambito di applicazione di queste norme riguarda il trattamento dei dati personali, definiti come "qualsiasi informazione concernente una persona fisica identificata o identificabile; si considera identificabile la persona che può essere identificata direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o a più elementi specifici caratteristici della identità fisica, fisiologica, psichica, economica, culturale o sociale". Tra tali dati rientrano quindi sia i dati anagrafici di una persona (ad

[20] Nonno, F., *Le normatuve sulla privacy*, Il notiziario tecnico Telecom Italia.

esempio nome e cognome) che quelli riconducibili alla stessa persona, quali ad esempio il codice fiscale, il numero telefonico, la carta di credito, ecc.

Al trattamento dei dati personali si applicano una serie di principi (ad esempio, quelli di finalità, pertinenza e non eccedenza, aggiornamento), regole e misure di sicurezza.

Altro aspetto qualificante della normativa europea è costituito dalle tutele poste al trasferimento dei dati personali all'esterno dell'Unione Europea. Tale trasferimento è consentito solo verso i pochi Stati cui la Commissione Europea ha riconosciuto un livello di protezione dei dati personali equivalente a quello comunitario oppure mediante l'adozione di determinate misure.

In particolare, per il trasferimento verso gli Stati Uniti vige il regime di "Safe Harbor", applicabile ai trasferimenti di dati verso aziende stabilite negli Stati Uniti che abbiano aderito a tale regime adottando volontariamente determinate misure per la protezione dei dati personali, sotto il controllo della Federal Trade Commission.

A distanza di tanti anni dall'adozione della "Direttiva madre", è possibile affermare che i principi in essa contenuti risultano tuttora validi, ma al contempo vanno riconosciuti alcuni punti di debolezza derivanti soprattutto dallo sviluppo di nuove tecnologie (esempio internet), che hanno reso sempre più facile ed immediata la circolazione dei dati a livello internazionale. L'aspetto più delicato in questo senso è rappresentato dalla diversa trasposizione delle norme comunitarie da parte degli Stati membri: l'assenza di armonizzazione nell'ambito dell'Unione Europea ha rappresentato il limite più evidente.

4.2 La Francia

Oltralpe esiste fin dal 6 gennaio 1978 la "Loi informatique e libertés", nella quale si afferma il principio per il quale chiunque intenda effettuare trattamenti di dati personali (i.e. nominativi) deve previamente notificarlo alla Commission Nationale Informatique et Libertés. Come sappiamo il principio della notifica preventiva dei trattamenti dei dati personali è stato introdotto anche nella Direttiva 46/95/CE e, conseguentemente, anche nella legge 675/96.

La legge si applica indipendentemente dalla circostanza che il trattamento venga effettuato da soggetti francesi o stranieri, essendo l'applicazione stessa basata su un principio "territoriale", adottato anche dalla legge 675/96. In base a tale principio, l'applicazione della legge dipende dalla circostanza che il trattamento venga effettuato nel territorio dello Stato, indipendentemente, dunque, dalla nazionalità dei soggetti coinvolti in detto trattamento.

La legge francese si applica anche agli archivi manuali, ma solo ove gli stessi siano in qualche modo connessi ad archivi automatizzati. Essa inoltre non si applica ai dati personali relativi alle persone giuridiche. Ricordiamo che l'estensione dell'ambito di applicazione della legge agli archivi manuali e alle persone giuridiche costituiva una delle opzioni tra le quali la Direttiva consentiva agli Stati membri di scegliere in sede di attuazione. Con la legge 675/96, lo Stato italiano ha optato per l'estensione della normativa sia agli archivi manuali che ai dati relativi a persone giuridiche e non solo fisiche.

La normativa francese si applica tanto ai trattamenti effettuati da enti privati che a quelli effettuati da enti pubblici. Un importante spunto di riflessione è dato dalla previsione, nella normativa francese, di disposizioni anche più restrittive nei confronti dei trattamenti effettuati nell'ambito pubblico (necessità di espressa autorizzazione del CNIL), circostanza d'altra parte comprensibile e facilmente spiegabile, se si pensa a quanto potenzialmente più pericolosi per la privacy dell'individuo possano essere gli archivi pubblici rispetto a quelli privati. La legge italiana, al contrario, prevede restrizioni per così dire "a monte" (l'autorizzazione della legge al trattamento di dati sensibili da parte di soggetti pubblici), ma non impone particolari oneri successivamente (autorizzazione specifica da parte dell'autorità di controllo).

4.2.1 La nuova legge e il caso Google

Dopo il parere favorevole del Consiglio costituzionale, la Francia ha promulgato la nuova legge sulla protezione dei dati (n. 2004 - 801) che recepisce pienamente la Direttiva comunitaria 95/46/CE.

Rispetto alla precedente legge, che risale al 1978, il nuovo testo aumenta i poteri sanzionatori dell'autorità di protezione dati (CNIL), elimina l'obbligo di notificazione per i titolari che nominano un referente per la protezione dei dati e dispone l'obbligo di sottoporre a valutazione preliminare da parte della CNIL qualsiasi trattamento che comporti il ricorso a tecniche biometriche.

All'esito di un lungo e tormentato iter legislativo, durato oltre 2 anni ed iniziato in ritardo rispetto al termine di recepimento previsto dalla Direttiva comunitaria (24 ottobre 1998), il Parlamento francese ha licenziato la nuova legge sulla protezione dei dati destinata a sostituire la "Loi Informatique et Libertè".

A proposito di poteri sanzionatori, vale la pena ricordare la multa di 150 mila euro comminata dal CNIL al colosso Google, reo di non aver rispettato le regole francesi in materia di protezione dei dati personali. A non piacere al CNIL è stata la modifica apportata a marzo 2012 da Google alla policy in materia di privacy, in base alla quale Mountain View può condividere i dati raccolti su uno dei suoi servizi con tutti gli altri servizi utilizzati dallo stesso utente: se questa aggregazione di informazioni permette a Google di offrire prodotti ritagliati sulle esigenze del singolo utente (suggerimenti di ricerca basati per esempio su geolocalizzazione ottenuta attraverso Maps o video visti su YouTube), gli permette altresì di schedarlo in maniera abbastanza precisa, a favore degli inserzionisti.

A Google si rimprovera di non aver correttamente informato gli utenti delle modifiche introdotte nelle condizioni d'uso, né di come e perché i loro dati vengono raccolti, mancando inoltre di ottenere il loro consenso esplicito. Infine, l'autorità francese ritiene che Big G non rispetti l'obbligo relativo alla pubblicazione del periodo massimo di conservazione dei dati raccolti in questo modo[21].

4.3 La Spagna

[21] Tamburrino C., punto-informatico.it, 10/01/2014.

L'ordinamento spagnolo presenta alcune peculiarità in materia di protezione dei dati personali, che ne evidenziano la originalità rispetto al resto degli ordinamenti europei. Infatti, la tutela della riservatezza è riconosciuta a livello costituzionale, dall'art. 18 della Costituzione adottata nel 1978, il cui quarto comma prevede che un'apposita legge "porrà limiti all'uso dell'informatica per salvaguardare l'onore e l'intimità personale e familiare dei cittadini e il pieno esercizio dei loro diritti". Peraltro, va sottolineato come i precedenti commi dello stesso articolo garantiscano il diritto all'onore, all'intimità personale e familiare e all'immagine, la inviolabilità del domicilio e il segreto delle comunicazioni.

Le previsioni "programmatiche" contenute nell'articolo 18 della Costituzione spagnola sono state attuate con l'adozione di leggi apposite: quella del 1982 sull'onore, quella del 1984 sulle intercettazioni telefoniche, ripresa nel 1992 dalla cd. "Legge Corcuera" sulla sicurezza urbana. Per molto tempo l'unica parte dell'articolo 18 rimasta inattuata è stato proprio il quarto comma: solo il 31 gennaio del 1993 è entrata in vigore la "Legge organica per regolare il trattamento automatizzato di dati personali" (LORTAD). Si tratta di una legge organica, cioè di una legge di rango superiore rispetto a quella ordinaria, paragonabile alle nostre leggi costituzionali, dalle quali si discosta tuttavia per alcune peculiarità che non è dato rinvenire nell'ordinamento italiano. La stessa costituzione spagnola stabilisce che la legge organica va approvata globalmente e dalla maggioranza assoluta del congresso. La legge organica, inoltre, si caratterizza per la circostanza che essa può contenere disposizioni con il valore di legge ordinaria, al fine di renderne alcune parti più facilmente modificabili.

Un altro elemento che rende l'esperienza spagnola alquanto originale è stata la particolare sensibilità dimostrata dall'opinione pubblica e dai privati con riguardo ai problemi della tutela della riservatezza nell'era informatica. Nel novembre del 1990 fu istituita, su iniziativa di un gruppo di privati, la Commissione per le Libertà e l'Informatica (CLI) . Infatti, in occasione di un censimento, molti cittadini avevano rilevato che alcune delle domande contenute nel questionario risultavano eccessivamente penetranti: il timore che si diffuse era quello che i dati venissero utilizzati non tanto a fini statistici, bensì a fini fiscali. In assenza di un organo pubblico di controllo del settore relativo al trattamento dei dati personali, un gruppo di soggetti privati composto da associazioni di magistrati, lavoratori, operatori di marketing, tecnici dell'informazione, utenti di tecnologie informatiche, ecc., decise di dare vita a questo organismo, attualmente ancora attivo e che, a partire dal 1997, opera come sezione specializzata della Associazione Spagnola per i Diritti Umani. Scopo principale della CLI è quello di promuovere in tutto il Paese "la protezione dei diritti dell'individuo, in particolare il diritto all'intimità, nei confronti delle tecnologie informatiche e della comunicazione, cercando di sensibilizzare l'opinione pubblica sull'importanza di questi temi per lo sviluppo e il rafforzamento della democrazia in una società tecnologica".

Attualmente, la legge organica del 1993 è stata sostituita dalla legge n. 15 del 1999 (sempre organica), con la quale è stata data attuazione anche in Spagna alla Direttiva europea del 25 ottobre 1996 (95/46/CE).

Anzitutto, la legge spagnola si distingue dalla legge 675/96 con riguardo al suo oggetto e al suo ambito di applicazione. La legge organica, infatti, garantisce e protegge, rispetto al trattamento di dati personali "le

libertà pubbliche e i diritti fondamentali delle persone fisiche, con particolare riguardo all'onore e l'intimità personale e familiare". Pertanto, la legge non trova applicazione per le persone giuridiche, a differenza di quella italiana, il cui articolo 1 la dichiara espressamente applicabile anche nei confronti "delle persone giuridiche e di ogni altro ente o associazione".

Con riguardo al proprio ambito di applicazione, mentre la legge italiana disciplina i trattamenti effettuati sul territorio italiano, la legge spagnola, oltre ad applicarsi ai trattamenti di dati effettuati sul territorio nazionale, specifica che essa troverà applicazione anche quando il responsabile del trattamento si trovi fuori del territorio spagnolo ma, in base alle norme di diritto internazionale privato, gli si debba applicare la legge spagnola ovvero quando il responsabile si trovi fuori del territorio europeo e utilizzi per il trattamento mezzi situati in Spagna, salvo che tali mezzi siano utilizzati esclusivamente in via transitoria. Si noti che per "responsabile", secondo la legge spagnola, si intende la figura corrispondente al nostro "titolare", vale a dire il soggetto cui competono le decisioni relative alle finalità, contenuto e uso del trattamento – anche, se come vedremo, poiché la legge spagnola introduce anche il concetto di archivio, colui che crea l'archivio, può non coincidere con il responsabile così inteso. L'"incaricato" spagnolo, d'altra parte, corrisponde al "responsabile" italiano, cioè colui che effettua il trattamento per conto del titolare. Sono esclusi dall'ambito di applicazione della legge: gli archivi personali o domestici, gli archivi sottoposti a segreto di Stato, gli archivi realizzati per investigazioni sul terrorismo e sulla criminalità organizzata.

Quanto ai principi generali, analogamente a quanto previsto dalla normativa italiana, i dati devono essere adeguati, pertinenti e non eccedere le finalità del trattamento, il quale non potrà essere effettuato per finalità diverse da quelle dichiarate al momento della raccolta. Anche secondo la legge spagnola, è necessario fornire all'interessato alcune informazioni al momento della raccolta dei dati, in particolare sull'esistenza di un archivio che ne contiene i dati personali, sulla natura obbligatoria o facoltativa della comunicazione dei propri dati e sulle conseguenze di un eventuale rifiuto, sulla possibilità di esercitare i propri diritti (di accesso, rettifica, cancellazione e opposizione), sulle generalità del responsabile.

Il trattamento di dati personali potrà essere effettuato solo con il consenso "inequivoco" dell'interessato, salvo che la legge disponga diversamente. E la stessa legge organica introduce una serie di eccezioni, simili a quelle previste dalla legge italiana. Inoltre, il consenso può essere in qualsiasi momento revocato, in presenza di una giusta causa.

Vengono considerati "dati sensibili" i dati personali che rivelano le convinzioni ideologiche, l'appartenenza sindacale, religiosa o filosofica dell'interessato. Per il trattamento di questi dati la legge organica richiede il consenso espresso e scritto dell'interessato. I dati riguardanti l'origine razziale, la salute, la vita sessuale potranno essere oggetto di trattamento con il consenso espresso dell'interessato ovvero quando, per ragioni di interesse generale, una disposizione di legge le consenta.

Per quanto riguarda il profilo della sicurezza, la legge organica impone al responsabile l'obbligo di adottare le misure necessarie, tenendo conto dello stato della tecnologia, la natura dei dati e i rischi a cui sono esposti.

Inoltre, la legge spagnola sancisce l'obbligo del segreto professionale a carico del responsabile e di chiunque intervenga in una qualsiasi fase del trattamento.

Quanto alla comunicazione dei dati personali, questa potrà essere effettuata solo con il consenso dell'interessato, salve alcune eccezioni (previsione di legge, dati accessibili al pubblico, comunicazione alle autorità fiscali o giudiziarie, o alle amministrazioni pubbliche per fini statistici, storici, o scientifici, dati sanitari da comunicare per fronteggiare una urgenza o per realizzare studi). La legge organica sancisce la nullità di detto consenso nel caso in cui l'interessato non sia stato messo nelle condizioni di conoscere le finalità del trattamento o il tipo di attività nel cui ambito avverrà la comunicazione. Anche in questo caso il consenso è revocabile.

4.3.1 Archivi pubblici e privati

Anche la legislazione spagnola prevede una disciplina differenziata per gli archivi pubblici e per quelli privati.

Con riguardo agli archivi di titolarità pubblica, la loro creazione, modifica o soppressione può avvenire solo in base ad una disposizione di legge che indichi chiaramente le finalità, gli interessati i cui dati personali saranno raccolti, il procedimento di raccolta e la struttura dell'archivio, eventuali cessioni di dati, l'organo responsabile, le modalità per l'esercizio dei diritti dell'interessato, le misure di sicurezza adottate. Ci sono numerose eccezioni a favore delle amministrazioni pubbliche: a) i dati possono essere comunicati ad altre amministrazioni quando lo dispone una norma di legge; b) la polizia può effettuare trattamenti di dati sensibili in base al criterio della "necessità delle indagini in corso"; c) in base allo stesso criterio è possibile escludere il diritto di accesso, rettifica, cancellazione, come anche nel caso in cui l'accesso rappresenti un ostacolo all'adempimento di obblighi fiscali o quando l'interessato sia oggetto di attività ispettiva; d) è possibile non rendere l'informativa all'interessato al momento della raccolta quando ciò possa ostacolare o impedire le funzioni di controllo nel caso di illeciti amministrativi.

Quanto agli archivi di titolarità privata, anche la legge spagnola introduce l'obbligo a carico di chi crea un archivio di dati personali (che dunque sembra potere essere persona diversa dal responsabile) di notificarlo alla Agenzia per la protezione dei dati (APD). Si noti come la normativa spagnola, pur disciplinando il "trattamento" di dati personali, in moltissime occasioni ha come oggetto non il trattamento, ma l'archivio di dati personali. Da questo punto di vista, la legge spagnola si distingue da quella italiana, secondo la quale è il trattamento ad essere oggetto di notifica, autorizzazione, esenzione, mai l'archivio o la banca dati, di cui si può parlare solo in relazione ai "trattamenti" dei dati ivi contenuti. Forse l'approccio spagnolo potrà sembrare meno coerente, ma, dal punto di vista pratico, è più facile collegare un obbligo come quello della notifica, ad esempio, alla creazione dell'archivio piuttosto che ai trattamenti ad esso connessi, che possono essere anche innumerevoli e meno facili da controllare.

Nella sezione dedicata agli archivi privati, singole disposizioni si preoccupano di disciplinare in dettaglio alcune ipotesi particolari: a) la cessione di dati da parte del responsabile dell'archivio, che deve essere

comunicata all'interessato; b) il trattamento di dati accessibili al pubblico in quanto facenti parte di liste pubbliche; c) gli archivi contenenti informazioni sulla solvenza patrimoniale e sul credito; d) i trattamenti effettuati a fini di marketing, che potrà essere effettuato solo su dati accessibili al pubblico o con il consenso dell'interessato. Un'altra peculiarità della legislazione spagnola è data dal cosiddetto Censo Promocional. Le aziende che operano nel settore del marketing diretto, della pubblicità, della vendita a distanza, possono chiedere all'Istituto nazionale di statistica una copia di tale lista, che è formata dai nomi, cognomi e indirizzi dei soggetti inseriti nelle liste elettorali. I cittadini hanno il diritto di farsi cancellare da questa lista. La lista potrà essere utilizzata per un anno, decorso il quale perderà la sua qualità di fonte accessibile al pubblico – che è una condizione essenziale per effettuare alcuni dei suindicati trattamenti senza ottenere il consenso dell'interessato.

Quanto al trasferimento di dati all'estero, la legge organica lo ammette solo nel caso in cui il paese destinatario dei dati preveda un livello di protezione equiparabile a quello previsto dalla stessa legge organica, a meno che non si ottenga l'autorizzazione da parte dell'APD, la quale provvederà a rilasciarla solo se saranno state ottenute adeguate garanzie. Ci sono alcune eccezioni a questo principio generale, la più rilevante delle quali è la circostanza che destinatario del trasferimento sia uno Stato membro dell'Unione europea ovvero uno Stato terzo, la cui legislazione sia stata ritenuta adeguata dalla Commissione europea.

4.3.2 L'autorità di controllo

L'APD è l'organo di diritto pubblico preposto alla vigilanza del settore relativo alla protezione dei dati personali, al quale sono demandate tutta una serie di attività funzionali all'applicazione della legge: rilasciare le autorizzazioni necessarie, esaminare i reclami degli interessati, eseguire ispezioni sugli archivi oggetto della legge organica, l'emanazione delle sanzioni. L'apparato sanzionatorio predisposto dalla legge organica, non prevede che sanzioni pecuniarie a carico dei responsabili, a differenza di quello italiano, il quale introduce sanzioni penali piuttosto rilevanti, e per questo motivo è stato oggetto di numerose critiche.

4.4 La Gran Bretagna: la legge di seconda generazione

Dal 1 Marzo 2000 la tutela dei dati personali in Gran Bretagna è disciplinata dal Data Protection Act 1998 in attuazione della direttiva 95/46/CE . La nuova legge, che è completata da ben 17 regolamenti di attuazione, rafforza ed estende il regime di tutela dei dati personali che in Gran Bretagna era previsto sin dal Telecommunications and Data Protection Act del 1984.

In particolare, l'ambito di applicazione della legge viene esteso anche a certe forme di archivi manuali, mentre il data subject (ovvero il soggetto cui si riferiscono i dati personali) gode di una tutela più estesa e le procedure di registrazione vengono sostituite con procedure di notificazione. Sono riaffermati i principi di qualità nel trattamento, si prevedono condizioni più stringenti per il trattamento di certi dati particolari (ad esempio quelli "sensibili") insieme a nuove regole per il trasferimento dei dati a Paesi fuori dall'UE.

Infine, risultano rafforzati i poteri dell'Autorità garante. Questa era originariamente denominata Data Protection Registrar (1984), poi Data Protection Commissioner (1998) e, dal 30 gennaio 2001, Information Commissioner .

4.4.1 Il sistema normativo

Finalità principale del Data Protection Act 1998 era quella di adeguare la normativa inglese sulla privacy (Data Protection Act 1984) alle disposizioni della direttiva del '95, in tal modo allineandosi, per così dire, agli standard europei in tema di tutela dei dati personali.

Dal confronto tra l'attuale normativa inglese e quella italiana, emerge tuttavia che, anche dopo l'attuazione della direttiva, permangono alcune differenze, a volte anche significative, tra le discipline sulla privacy dei diversi Paesi europei.

La legge inglese si applica esclusivamente ai dati personali delle persone fisiche, mentre la legge 675/96, prevede, all' art. 1 , che la stessa trovi applicazione nei confronti "delle persone giuridiche e di ogni altro ente o associazione".

Vale, anche in Gran Bretagna, il principio della territorialità, per cui la legge sulla privacy trova applicazione rispetto ai trattamenti di dati effettuati sul territorio nazionale, ma con la precisazione che la legge inglese si applica anche laddove il trattamento sia effettuato da un soggetto non stabilito sul territorio nazionale che ricorre, ai fini del trattamento di dati personali, a strumenti situati nel territorio nazionale, a meno che questi non siano utilizzati ai soli fini di transito nel territorio nazionale. In quest'ultima ipotesi il titolare del trattamento è tenuto a nominare un rappresentante stabilito in Gran Bretagna.

Infine, le differenze esistenti circa il trattamento rilevante ai fini dell'applicabilità della legge sono venute meno proprio con la riforma del 1998 che ha esteso la tutela anche a certe forme di archiviazione manuale precedentemente escluse.

4.4.2 I diritti dell'interessato

Il Data Protection Act 1998, part II, attribuisce all'interessato il diritto di accesso ai dati oggetto del trattamento, conformemente all'art. 12 della Direttiva, il diritto di opporsi al trattamento di dati che sia o possa risultare pregiudizievole per l'interessato o per una terza persona, il diritto di opporsi al trattamento di dati condotto per scopi di direct marketing e il diritto a non essere sottoposta a decisioni individuali automatizzate ai sensi dell'art. 15 della direttiva.

Il consenso dell'interessato, che pure è richiesto dalla legge inglese quale condizione per il trattamento dei dati personali, non viene previsto nel corpo della legge, come avviene per la 675/96, bensì nell'allegato (Schedule 2). Così come in allegato sono affermati i principi di qualità nel trattamento dei dati personali (Schedule 1). L'impressione di chi scrive è che in tal modo si perde l'importanza chiave dei principi di qualità nel trattamento dei dati e della necessità del consenso al trattamento.

4.4.3 Gli obblighi del titolare

Il titolare del trattamento dei dati è tenuto a notificare al Commissioner i dati che lo riguardano e a fornire una descrizione generale delle misure di sicurezza adottate, nonché a comunicare le eventuali modifiche che dovessero intervenire successivamente. In certi casi particolari, quando il trattamento dei dati può apparire pregiudizievole, il titolare è tenuto ad astenersi dall'effettuare il trattamento dei dati fino a che il Commissioner non si sia pronunciato sulla notifica, ovvero non sia scaduto il termine dei 28 giorni entro i quali il Commissioner deve esaminare la notifica.

4.4.4 Le autorità garanti della protezione dei dati personali

Due sono le autorità preposte alla tutela dei dati personali in Gran Bretagna: il Data Protection Commissioner e il Data Protection Tribunal .

Il Data Protection Commissioner riceve le notificazioni dei titolari del trattamento di dati personali, ne cura la registrazione e mantiene il registro dei titolari. Le informazioni contenute nel registro sono accessibili al pubblico gratuitamente e senza particolari limiti; dietro retribuzione, è possibile chiedere copia certificata delle informazioni.

Il Commissioner effettua un controllo preventivo circa le notificazioni riguardanti trattamenti di dati che sono o potrebbero essere pregiudizievoli per l'interessato e, entro un periodo di 28 giorni, peraltro prorogabile, invia le proprie conclusioni. Il Commissioner vigila sulla corretta applicazione della legge sulla privacy e invia, nei casi opportuni, notificazioni ai titolari. Ha inoltre funzioni propositive e consultive relativamente ai regolamenti disciplinanti il procedimento di notifica.

Dal 30 Gennaio 2001 il Data Protection Commissioner ha assunto il ruolo di garante della libertà di informazione ed è ora noto come Information Commissioner .

Il Data Protection Tribunal composto di membri togati e non togati, (questi ultimi rappresentano gli interessi delle parti in conflitto, ovvero titolari e interessati), è competente a conoscere i reclami avverso le decisioni del Data Commissioner . Va sottolineato come in questo caso, a differenza del caso italiano, le competenze giurisdizionali in materia di dati personali siano state attribuite ad un organo di natura giudiziaria che non coincide con l'organo di controllo.

4.5 Gli Stati Uniti

Ad oggi, due principali approcci alla regolamentazione in materia di privacy sono prevalenti negli USA. Il primo si basa sulle cosiddette “fair information practices”, che prevedono come elementi fondamentali l’informativa e la capacità di scelta dell’interessato. Si tratta di un approccio che prende in considerazione il processo che porta al trattamento dei dati ed è esemplificato dal cosiddetto GLBA (Gramm-Leach-Bliley Act). Tale norma rimosse le barriere poste da leggi previgenti alla fusione tra le attività economiche di società operanti in diversi settori finanziari, come banche e assicurazioni. La possibilità di trasferire

informazioni tra questi diversi soggetti economici creò preoccupazioni nell'opinione pubblica per la tutela della privacy dei cittadini, tanto che pochi anni prima dell'approvazione del GLBA, erano venuti alla luce dei casi di pratiche illecite. In particolare, erano state scoperte alcune importanti istituzioni finanziarie che vendevano dettagliate informazioni sui propri clienti a società di telemarketing, che poi utilizzavano per addebitare a clienti inconsapevoli servizi non richiesti. Il caso più clamoroso riguardò la US Bancorp e l'azienda di telemarketing MemberWorks e terminò con un'ammenda di 3 milioni di dollari inflitta alla banca per frode e pratiche commerciali scorrette. Di conseguenza, furono inserite nel GLBA specifiche disposizioni a tutela dei dati personali, che in sintesi riguardano l'adozione di misure per la sicurezza dei dati, l'obbligo di informare il cliente riguardo le policy di comunicazione dei suoi dati personali a terze parti e la sua possibilità di opporsi alla condivisione dei suoi dati finanziari con terze parti.

Il secondo approccio prevalente negli USA è quello del cosiddetto "permissibile purpose", che limita il trattamento dei dati personali a determinate finalità, previste dalla legge; questo approccio prende quindi in considerazione il contesto in cui avviene il trattamento dei dati.

Il FCRA (Fair Credit Reporting Act), promulgato nel 1970, è una delle leggi sulla privacy in vigore da più tempo negli USA e costituisce il miglior esempio di attuazione di questo approccio. Nell'America degli anni '60 era diffusa tra i commercianti la prassi dello scambio di informazioni relative ai propri clienti ai fini della concessione di credito. In molti casi i cittadini si trovavano danneggiati a causa di informazioni imprecise, che peraltro essi non potevano né conoscere né correggere. Per risolvere tale situazione, il FCRA prevede che le cosiddette Credit Reporting Agencies garantiscano una ragionevole accuratezza delle informazioni relative al credito e le forniscano solo a soggetti che le trattano per finalità consentite (legittime attività economiche, gestione del rapporto di lavoro, obblighi di legge, ecc.). Inoltre gli interessati devono poter accedere alle informazioni che li riguardano ed hanno il diritto di essere informati qualora sulla base di tali informazioni siano prese decisioni negative, ad esempio negando un finanziamento.

In generale quindi, le leggi degli Stati Uniti mirano a regolamentare il trattamento dei dati personali in specifici ambiti di attività economica, nella misura in cui vi possano essere rischi per il consumatore. Ne deriva che negli Stati Uniti, differentemente dall'Europa (come di seguito descritto), la privacy non costituisce un diritto fondamentale dell'individuo, ma è un diritto del consumatore, da bilanciare con le esigenze di business delle imprese.

In linea con questa impostazione, negli Stati Uniti non esiste una specifica autorità incaricata della tutela dei dati personali dei cittadini, equivalente ad esempio al Garante privacy italiano. La FTC (Federal Trade Commission), che è la principale agenzia incaricata della tutela dei consumatori negli Stati Uniti, vigila anche sull'aderenza dei comportamenti delle aziende a quanto esse dichiarano nelle proprie privacy policy e sul rispetto delle leggi in materia di privacy. Al riguardo, occorre notare che il potere di controllare il corretto adempimento di obblighi normativi deve essere previsto dalle leggi stesse, mentre il potere di vigilare sull'applicazione delle privacy policy definite dalle aziende è insito nella legge istitutiva della FTC

(il cosiddetto FTC Act). Infatti la FTC ha, tra l'altro, il compito di contrastare le pratiche commerciali scorrette, cioè dannose per il consumatore e "ingannevoli" (basate su informazioni false).
Peraltro le azioni promosse dalla FTC non precludono indagini anche da parte dell'autorità giudiziaria.

CONCLUSIONI

Il tema della privacy è di vecchia data ma è esploso negli anni recenti con il fiorire della società tecnologica. L'idea di trattare l'argomento in un'ottica analitica piuttosto ampia che abbracciasse contesto normativo e problematiche concrete ha preso forma consistente attraverso le semplici dinamiche quotidiane, ovvero sull'osservazione attente dell'impatto che ha sulla vita di tutti i giorni quest'entità apparentemente conosciuta, ma in fondo non meglio definita, che è appunto la Privacy.

Se è vero infatti che la possibilità di dare la forma che vogliamo alla nostra vita passa attraverso il controllo delle informazioni che ci riguardano, della nostra immagine, di ciò che vogliamo tenere per noi e di ciò che invece vogliamo che sia pubblico, basta ascoltare amici per strada che si danno appuntamento per il pomeriggio su un social network e magari si raccomandano di non pubblicare una foto compromettente scatta ad una festa o, al contrario, ridono dello sprovveduto di turno le cui foto hanno finito con l'essere diffuse lontano dal luogo in cui lui credeva ingenuamente di averle lasciate; oppure pensare ai numerosi articoli letti sui giornali o nel web in cui si raccontano con curiosità contenuti – magari tutt'altro che di pubblico interesse – solo a discapito della dignità di un interessato oggetto di una nuova illecita intercettazione ambientale o, approccio opposto, si grida allo scandalo se nell'ambito di intercettazioni lecite da parte delle AA.GG. viene coinvolto un personaggio che non sarebbe dovuto comparire; o ancora sentirsi rivolgere da parte di un impiegato a uno sportello (di un ufficio pubblico o privato che sia) la richiesta di firmare un'informativa e di tracciare alcune non meglio specificate "X" ai fini della fruizione del servizio. Questa è la privacy nel quotidiano e gli esempi potevano continuare all'infinito.

E’ acclarato come ormai sia sempre più indispensabile considerare la sicurezza dei dati un fattore critico sia a tutela del business che di aspetti esclusivamente legati alla vita privata dei comuni cittadini. Avendo i comuni strumenti tecnologici un impatto globale, una reale tutela della persona dovrebbe continuare ad essere comunque ricercata nell’ambito di un più ampio strumento giuridico universale, idoneo a sostenere i fondamentali principi di libertà: in altre parole, una sorta di Bill of Right[22].

BIBLIOGRAFIA

[22] Nel summit mondiale di Tunisi del 2005 è stata formulata per la prima volta la proposta di Internet Bill of Rights definito come un processo continuo basato sui diritti fondamentali esistenti ed orientato a promuovere sia la loro applicazione che il riconoscimento di ulteriori principi e diritti, i quali a loro volta includano, fra gli altri, i temi della privacy, della protezione dei dati, della libertà di parola, dell’accesso universale, della neutralità della rete, dell’interoperabilità, della possibilità di raggiungere tutti i nodi Internet, dell’uso di formati e standard aperti, dell’accesso pubblico alla conoscenza, del diritto ad innovare, così come delle regole del mercato libero (fra le quali il diritto ad un mercato on-line giusto e competitivo ed i diritti dei consumatori in generale).

AA.VV., *Codice della privacy*, commento al decreto legislativo 30 giugno 2003, n. 196, Giuffrè, Milano, 2004.

R. Acciai, (a cura dì), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Maggioli, Rimini, 2004.

G. Arcudi, V. Poli, *II diritto alla riservatezza*, Ipsoa, Milano, 2000.

E. Barila, C. Caputo, *La tutela della privacy nella pubblica amministrazione*, Milano, Giuffrè, 2000.

F. Berghella, *Guida pratica alle misure di sicurezza e ai controlli per la privacy: gli adempimenti per le banche e le finanziarie*, Bancaria Editrice, 2000.

F. Bilotta, *L'emersione del diritto alla privacy*, in A. Clemente (a cura di), Privacy, Cedam, Padova, 1999.

G. Branca, G. Alpa, *Istituzioni di diritto privato*, Zanichelli, Bologna, 1992.

G. Buttarelli, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, Giuffrè, Milano, 1997.

N. Bobbio, *L'età dei diritti*, Einaudi, Torino, 1990.

F. Cardarelli, S. Sica, V. Zeno-Zencovich, *Il codice dei dati personali: Temi e problemi*, Giuffrè, Milano, 2004.

G. Cassano, S. Fadda, *Codice in materia di protezione dei dati personali. Commento articolo per articolo al testo unico sulla privacy*, Ipsoa, Milano, 2004.

G. Cassano, M. Del Vecchio, *Il diritto alla riservatezza e accesso ai documenti amministrativi*, Giuffrè, Milano, 2001.

G.P. Cirillo, *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Giuffrè, Milano, 2004.

Clemente, (a cura di), *Privacy*, Cedam, Padova, 1999.

V. Cuffaro, V. Ricciuti (a cura di), *La disciplina del trattamento dei dati personali*, Giappichelli, Torino, 1997.

De Cupis, *Riservatezza e segreto*, (diritto a), in Novissimo Digesto Italiano XVI, Torino, 1969.

G. Elli, R. Zallone, *Il nuovo codice della privacy*, (commento al d. Lgs. 30 giugno 2003, n. 196 con la giurisprudenza del Garante), Giappichelli, Torino, 2004.

V. Frosini, *Banche dati, telematica e diritti delle persone*, Cedam, Padova, 1981.

V. Frosini, *Informatica, diritti e società*, Cedam, Padova, 1992.

E. Giannantonio, G. Losano, V. Zeno- Zencovich, (a cura di), *La tutela dei dati personali. Commento alla legge n. 675/96*, Cedam, Padova, 1999.

R. e R. Imperiali, *La tutela dei dati personali, Commento alla normativa sulla protezione dei dati personali*, Il sole 24, Milano, 2004.

R. e R. Imperiali, *La tutela dei dati personali. Vademecum sulla privacy informatica*, Il sole 24 ore, Milano, 1997.

S. Labriola, *Le autorità indipendenti. Da fattori evolutivi ad elementi della transazione nel diritto pubblico italiano*, Giuffrè, Milano, 2000.

T. Minella, *La privacy. Giuda alla applicazione della legge 675/96*, Ed. Simone, Milano, 1997.

Mucio, *Il diritto alla riservatezza nella pubblica amministrazione: dati sensibili, dati personali e diritto di accesso*, Ipsoa, Milano, 2003.

R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003.

S. Rodotà, Tecnopolitica. *La democrazia e le nuove tecnologie della comunicazione*, Editori Laterza, Bari - Roma, 2004.

S. Rodotà, *Intervista su privacy e libertà*, P. Conti(a cura di), Editori Laterza, Bari - Roma, 2005.

S. Rodotà, *Tecnologia e diritti*, Il Mulino, Bologna, 1995.

S. Rodotà, *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna 1973.

Tosi, *Il codice della privacy. Tutela e sicurezza dei dati personali, normativa nazionale e comunitaria*, La Tribuna, Piacenza, 2004.