



LEO STILO

**IL TRATTAMENTO DEI DATI
PERSONALI NELLA PUBBLICA
AMMINISTRAZIONE**

TRA INNOVAZIONE E RESPONSABILITÀ

Il Nuovo Diritto Sas di Leo Stilo & C.
Via Catone, 29 – 00192 Roma
Tel. 06-39737961 – Fax 06-23328225
www.ilnuovodiritto.com – info@ilnuovodiritto.com

© Copyright 2007 – Tutti i diritti riservati

Ai lettori della rivista Il Nuovo Diritto

INDICE

1. PREMESSE.....	9
2. L'INNOVAZIONE TECNOLOGICA DELLA PUBBLICA AMMINISTRAZIONE: DALLO STATO AUTORITARIO ALL'UMILE CITTADINO.....	11
3. IL RISCHIO E LE RESPONSABILITÀ DERIVANTI DALLA GESTIONE DEI DATI PERSONALI DA PARTE DELLA PUBBLICA AMMINISTRAZIONE.....	19
4. GENESI STORICA DI UN DIRITTO FONDAMENTALE DELL' "HOMO TECNOLOGICUS"	24
5. DALLA CONVENZIONE DI STRASBURGO AL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI.....	33
6. IL TRATTAMENTO DEI DATI PERSONALI NELLA PUBBLICA AMMINISTRAZIONE: I PRINCIPI GENERALI.....	43
7. DEFINIZIONE DI DATI PERSONALI, SENSIBILI, GIUDIZIARI ... E BIOMETRICI.....	51
8. L'ORGANIGRAMMA "PRIVACY": DEFINIZIONI, RESPONSABILITÀ E DELEGA DI FUNZIONI.....	57
9. L'INTERESSATO E I SUOI DIRITTI.....	70
10. IL TRATTAMENTO DEI DATI PERSONALI: LE REGOLE GENERALI E LE RESPONSABILITÀ DA TRATTAMENTO ILLECITO.....	81
11. LE ULTERIORI REGOLE PER IL TRATTAMENTO DEI DATI DA PARTE DEI SOGGETTI PUBBLICI.....	97

12. LA SICUREZZA DEI DATI PERSONALI NELL'AMBITO DELLA PUBBLICA AMMINISTRAZIONE TRA MISURE DI SICUREZZA E RESPONSABILITA'.....	106
13. LA PUBBLICA AMMINISTRAZIONE TRA DIRITTO DI ACCESSO E TRATTAMENTO DEI DATI PERSONALI.....	114
BIBLIOGRAFIA GENERALE.....	141
INDICE ANALITICO.....	146

1. PREMESSE

Affrontare il tema del trattamento dei dati personali nella pubblica amministrazione offre l'opportunità di compiere alcune riflessioni in merito ai mutamenti epocali intervenuti nei rapporti tra Stato e cittadino, tra governanti e governati. Le cause poste alla base di tali sconvolgimenti possono essere identificate, sinteticamente, nell'innesto nel DNA autoritario del diritto amministrativo di sequenze genetiche liberali contenute nella Costituzione, nel diritto comunitario e in numerose convenzioni internazionali e nell'impulso organizzativo e culturale determinato dal ruolo cruciale ed irrinunciabile che le nuove tecnologie informatiche rivestono nella moderna società. **Il diritto alla protezione dei dati personali diviene, nell'ambito della società dell'informazione, il punto di frizione e tenuta dello stesso ordinamento giuridico.** Il presente lavoro è diretto, quindi, ad esaminare in modo specifico la disciplina relativa al trattamento dei dati personali nell'ambito della Pubblica Amministrazione, con particolare attenzione ai momenti di responsabilità, attraverso una preventiva ricerca del fondamento giuridico del diritto alla protezione dei dati personali e del rapporto che tale diritto instaura tra lo Stato gestore dei dati e le persone a cui i dati si riferiscono. Infine, particolare attenzione è dedicata al

contemperamento nell'ambito della Pubblica amministrazione tra diritto alla tutela dei dati personali e diritto d'accesso alla documentazione amministrativa.

2. L'INNOVAZIONE TECNOLOGICA DELLA PUBBLICA AMMINISTRAZIONE: DALLO STATO AUTORITARIO ALL'UMILE CITTADINO

Il Codice dell'Amministrazione Digitale, la *Magna Charta* di una nuova realtà amministrativa (BERTONI), rappresenta il frutto maturo di una lunga e complessa riforma, in senso strutturale e culturale, della Pubblica Amministrazione italiana simbolicamente iniziata con la legge 7 agosto 1990, n. 241 ed ancora oggi in corso di attuazione. La riforma digitale della pubblica amministrazione trova fondamento nelle scoperte ed invenzioni tecnologiche nate dalla corsa verso le nuove tecnologie belliche, offensive e difensive realizzata durante gli anni del dopoguerra. I momenti più significativi di questo sviluppo tecnologico, che non ha ancora raggiunto la fase discendente della sua parabola evolutiva, sono rappresentati: dalla **microelettronica**, la cui nascita è collocabile, simbolicamente, nel 1947 nei Bell Laboratories di Murray Hill nel New Jersey dove venne inventato il *transistor* e con esso la possibilità di trasformare gli impulsi elettrici in un Codice binario utilizzabile, in estrema sintesi, per comunicare con le macchine in modo rapido e sempre più complesso; dal **computer**, strumento ormai paragonabile, per diffusione ed uso, ad un comune elettrodomestico, anch'esso

concepito dalla seconda guerra mondiale (madre di tutte le tecnologie); da **Internet** la cui ideazione e realizzazione rappresenta il frutto di una sinergica commistione tra la classica strategia militare e l'innovazione imprenditoriale di una nuova generazione di studiosi e ricercatori universitari. Sulla base dei tre mattoni appena citati (microelettronica, computer, internet) è oggi costruita la società dell'informazione in cui la stessa pubblica amministrazione, essendone parte, è costretta ad interagire e relazionarsi. Nel corso di questi ultimi anni si è sempre più di frequente considerato l'agire della Pubblica Amministrazione come il teatro di un inconciliabile e moderno conflitto interiore del diritto amministrativo. Tale reazione di rigetto è causata, come già evidenziato nelle premesse, dai principi liberali presenti nella Costituzione e nel diritto comunitario. Si è diffusa, tra gli studiosi e pratici del diritto, l'esigenza, quasi catartica, di rileggere attraverso le lenti dei principi liberali e democratici, acquisiti attraverso lunghi anni di complesse evoluzioni culturali, l'agire della Pubblica Amministrazione. La Pubblica Amministrazione deve rendere conto ai cittadini del suo operato e questi ultimi devono poter controllare l'esatto svolgersi delle dinamiche relative alla gestione della "cosa pubblica".

Tuttavia, nel sistema giuridico/sociale italiano è stata sempre diffusa, a partire da un livello che può essere definito epidermico

sino a quello più profondo ed intimo, **una concezione autoritaria** dello Stato in sé e del suo momento di incontro/scontro con i singoli individui che ne costituiscono l'aspetto sociale. L'intima natura dei rapporti tra chi detiene il potere, l'autorità governante, e chi è oggetto dell'esercizio del potere, i governati, in fondo non appare essere mutata nel corso dei secoli. La stessa rivoluzione francese, con le sue epocali conseguenze, è riuscita a colpire solo la struttura formale dell'antico regime senza modificarne la struttura sostanziale. La rivoluzione è riuscita a mettere da parte la figura del Re e la sua "sacra" icona; però, purtroppo, non è riuscita a scalfire la forza posta alla base della struttura rappresentativa che ha reso lo Stato una persona giuridica portatrice di interessi propri da realizzare attraverso forme di potere autoritario. Questa visione dei rapporti tra governanti e governati ha condotto inevitabilmente ad identificare lo Stato come un'entità portatrice di interessi diversi da quelli del singolo e della sua stessa collettività. L'atto amministrativo si configura così nella sua intima essenza come un chiaro momento di sintesi tra l'autorità del soggetto Pubblica Amministrazione e l'elemento volontaristico di derivazione privatistica comune ad ogni agire. La prima componente dell'atto amministrativo è connessa, per forza intrinseca e in modo indissolubile, all'idea di autorità intesa come: « ...il potere dell'uomo sull'uomo, e quindi individua una

posizione di supremazia che consente a taluno – al portatore di potere e dell'autorità, appunto – di imporre il proprio giudizio e più semplicemente la propria volontà agli altri.»(SATTA). Tale processo evolutivo appare legato alla nascita stessa dello Stato ed alla cosciente rinuncia ad un sistema di relazioni interpersonali di natura contrattuale, paritaria, a favore di un complesso apparato autoritario in cui il potere è delegato ad assemblee ristrette (oggi) o a singoli individui (nel passato). Si crea così un'entità nuova distaccata dalla società e dagli individui di cui essa è espressione di volontà; tale entità, divenendo detentrica del potere di gestire, programmare e realizzare l'interesse collettivo, lo attua tramite atti di volontà caratterizzati da un sacro alone d'autorità. «Immaginificamente e schematicamente si può dire che in un certo momento della storia, l'autorità morale di chi promuoveva il consenso dell'assemblea intorno alla propria proposta venne istituzionalizzata, con la creazione di un organo, dell'assemblea e della collettività; ma in quello stesso momento l'organo per ferrea legge di natura, cominciò anche ad avere vita propria, diversa e contrapposta alla vita della società.»(SATTA). Questo nuovo soggetto non si mette in relazione con la comunità e con i suoi singoli membri utilizzando quindi meccanismi di natura paritetica, ma adotta dei meccanismi che sono il riflesso della posizione di superiorità che ne costituisce l'intrinseca

antica essenza. Questa prima constatazione descrive, in modo intuitivo, solo una faccia della medaglia: lo Stato interagisce con gli individui (soci) attraverso strutture e con modalità autoritarie in cui la trasparenza e la possibilità di interazione da parte dei governati è pressoché inesistente o totalmente rilasciata all'iniziativa pubblica. La "personificazione" ha determinato lo scollamento tra lo Stato, ormai "persona autonoma" dotata di una vita e di fini propri, e la società consapevolmente costituita da individui eteronomi. Lo Stato, a causa di questo meccanismo culturale, viene posto ad un livello sovraordinato ai singoli. Lo stesso soggetto che amministra in nome dello Stato, o di una qualsiasi sua appendice burocratica, è dotato di una "qualità", pubblico ufficiale, che sembra elevarlo al di sopra di una qualsiasi altra persona comune anziché considerare tale posizione come un onere. Il diritto amministrativo, dopo secoli d'arroganza, si trova a dover compiere un atto d'umiltà e a ritornare ad esercitare una **funzione "modesta"** al servizio della collettività. «L'orizzonte concettuale in cui si svolge la teoria delle funzioni pubbliche viene, così, definitivamente spostato dallo Stato, colto nel momento in cui agisce per il perseguimento dei propri fini, all'ordinamento statale visto nella dinamica della sua propria attuazione. Ciò che ora diventa il necessario punto di riferimento per la qualificazione dell'attività pubblica non è più l'uno o l'altro scopo

dello Stato, ma la norma fondamentale regolatrice dell'ordinamento statale, a cui l'azione pubblica si riconnette e da cui prende slancio e direzione. In questo senso funzione pubblica è ogni attività che si costituisca come realizzazione dell'ordinamento, nella logica della produzione ed applicazione del diritto o anche di semplice obbedienza al diritto.» (MARONGIU). La sacralità può essere considerata un attributo solo della sovranità popolare e non dello Stato in sé e del suo supremo e indeterminato interesse pubblico. «Del resto, l'amministrazione negli ordinamenti contemporanei che si reggono sul principio di legalità non può essere nella sua essenza se non un'attività doverosa, che in tanto si legittima in quanto tende alla realizzazione dell'ordinamento di cui è funzione» (MARONGIU). Questa premessa di ordine generale sulla visione autoritaria dello Stato è necessaria per poter comprendere le difficoltà che oggi vive l'amministrazione pubblica nel tentativo di adeguarsi ad una rivoluzione che non è solo digitale ma anche e soprattutto culturale. La Pubblica Amministrazione non può più rimanere sorda alle richieste dei cittadini ma deve e può, alla luce degli strumenti tecnologici a sua disposizione, rendere dei servizi in modo economico ed efficiente rispettando le norme poste a tutela della persona e della sua dignità. **I servizi pubblici devono essere considerati appunto “servizi” e non momenti di autorità**

completamente avulsi dalla richiesta dei soggetti interessati che hanno il diritto di riceverli in modo rapido e corretto. Tuttavia, per modificare la visione autoritaria della Pubblica Amministrazione e rendere la stessa efficiente è stato necessario innovare i momenti più importanti della sua struttura e dei suoi procedimenti. Il primo settore da innovare necessariamente era quello dell'acquisizione, dell'archiviazione e della gestione dei documenti: linfa vitale di ogni settore dell'amministrazione pubblica. Quello che palesemente apparve non più procrastinabile era il bisogno di creare delle sinergie tra i vari settori e comparti della Pubblica Amministrazione, troppo spesso tra loro isolati a causa di una incomunicabilità atavica dovuta non solo a carenze strutturali ma anche e principalmente all'utilizzo di diversi "linguaggi" e procedure che rendevano le stesse amministrazioni pubbliche una comunità in cui i singoli soggetti parlavano e scrivevano utilizzando lingue e "velocità" diverse. È la legge 15 marzo 1997, n. 59 a rappresentare il vero punto di rottura con il passato e l'inizio di una profonda riforma culturale della Pubblica Amministrazione e dei suoi meccanismi documentali. Il "mattoncino" logico e giuridico su cui si è in breve tempo costruita una nuova concezione del "documento amministrativo", non più inscindibilmente legata ad una dimensione cartacea ma ad una natura squisitamente informatica, è rappresentato dall'art. 15, secondo

comma, della legge n. 59 del 1997: «Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge». Nel momento in cui l'informatica entra nella Pubblica Amministrazione snellendone i procedimenti e rendendo più rapide ed efficaci le ricerche documentali il primo passo verso un'amministrazione efficiente è stato compiuto. Il passo successivo è sicuramente quello di implementare l'interazione tra i diversi rami della amministrazione pubblica, ma ancora una volta il punto cruciale rimane quello di superare una **barriera culturale** che finché si ergerà forte nella mente di chi è chiamato a svolgere tali importanti servizi non consentirà una piena e compiuta riforma. Il fulcro su cui fare leva per sollecitare un rinnovamento capillare delle strutture amministrative è il diritto riconosciuto dall'art. 3 del Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005 n. 82):«**I cittadini e le imprese hanno diritto di ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni** e con i gestori di pubblici servizi statali nei limiti di quanto previsto nel presente Codice.»

3. IL RISCHIO E LE RESPONSABILITÀ DERIVANTI DALLA GESTIONE DEI DATI PERSONALI DA PARTE DELLA PUBBLICA AMMINISTRAZIONE

L'attacco alla visione autoritaria dello Stato, come già anticipato, è stato determinato da una lenta e costante opera di ampliamento e di affermazione dei diritti della persona nel rapporto intercorrente tra governanti e governati. Tra i diritti che più di altri appartengono alla sfera intima della persona vi è sicuramente quello relativo alla riservatezza ed al rispetto della vita privata. L'affermazione di questi diritti e il loro evolversi nell'ambito della società moderna in cui i rapporti e le relazioni interpersonali, reali e/o virtuali, sono basate sulla stessa informazione determina alcune problematiche piuttosto complesse. Il problema nasce nel momento in cui l'estrema libertà caratteristica delle nuove tecnologie della comunicazione si pone in rapporto con il diritto a vedere tutelati i propri dati personali utilizzati e sfruttati per scopi ignorati dall'utente. La diffusione di questa realtà rende evidente, con tratto grave, la difficoltà di perimetrare i confini che intercorrono tra la libertà di inviare/ricevere e cercare/trovare informazioni, da un lato, e la tutela della riservatezza della persona e dei dati ad essa appartenenti, dall'altro. La vasta zona d'ombra è provocata dal conflitto, difficilmente risolvibile con gli attuali strumenti giuridici, tra due contrapposte

esigenze, entrambe meritevoli di interesse e protezione da parte dell'ordinamento giuridico (GRIPPO): l'estremo vantaggio economico, sociale e culturale che la libera circolazione delle informazioni riesce a produrre; l'estremo rischio della riduzione del singolo individuo ad un ritratto virtuale ottenuto dal rinvenimento e dal trattamento di dati personali sparsi durante l'utilizzazione delle nuove tecnologie della comunicazione.

In particolare questa ultima considerazione si colora di particolari sfumature giuridico-amministrative alla luce del problema relativo all'applicabilità della normativa sulla tutela della riservatezza alle pubbliche amministrazioni. In base a tale necessità si contrappongono due esigenze: **il principio della trasparenza dell'azione amministrativa**, e quindi della pubblicità e conoscibilità degli atti delle pubbliche amministrazioni, sancito dalla legge n. 241/1990 e **il principio della tutela della riservatezza**. Come si può facilmente intuire entrambi i principi hanno rilevanza costituzionale essendo l'uno espressione dell'imparzialità e del buon andamento e l'altro della tutela dei diritti inviolabili della persona.

Il rischio di non poter controllare l'utilizzo dei dati personali utilizzati per "muoversi ed operare" nella società dell'informazione è congenito alla stessa natura delle tecnologie utilizzate.

Accanto alla capillare diffusione delle nuove tecnologie informatiche e telematiche è necessario diffondere in tutti i livelli della società **la consapevolezza dei costi e dei rischi ad essa connessi**. Mentre i rischi sono accettati come possibili, i costi da sopportare sono certi e non sono solo quantificabili in termini monetari, ma anche e principalmente in quantità di *privacy* da voler spendere e conservare. Questa consapevolezza deve essere ancora maggiore nell'ambito della Pubblica Amministrazione poiché la stessa si trova a fagocitare, per l'esercizio delle sue funzioni istituzionali, una serie infinita di dati ed informazioni relative a tutti i membri della società. Lo Stato inizia a registrare e trattare i dati dalla nostra nascita e continua a trattarli anche dopo la nostra morte. Se nel passato tutte queste informazioni si trovavano sparse fisicamente in archivi dislocati in posti fisicamente diversi ed era pressoché impossibile, se non investendo ingenti risorse, ricostruire ed organizzare i dati e le informazioni relative ad una persona, oggi questo ostacolo fisico e temporale non esiste più. **Le tecnologie informatiche applicate all'archiviazione e gestione delle informazioni non hanno creato effettivamente delle nuove conoscenze** che si vanno ad aggiungere alle precedenti inserite dalla mano dell'uomo, **ma** grazie alle elaborazioni delle preesistenti riescono a gestire in modo più incisivo, rapido e completo i dati

che hanno a disposizione. Ogni informazione, fisicamente inserita in tempi e luoghi diversi, nel momento in cui si aggiunge, affiancandosi, alle altre contenute nelle varie banche dati perde l'originale rapporto spazio-temporale con le precedenti e le successive per venire elaborata e trattata in funzione del suo intrinseco contenuto ed ordinata, di volta in volta, in funzione dell'interrogazione che l'utente, "cacciatore d'informazione", rivolge al sistema "elaboratore". Il *surplus* è dato dall'enorme vastità di notizie e nella capacità altamente selettiva che gli elaboratori elettronici mettono a disposizione dell'utente. La novità, quindi, risiede nella capacità di trovare in tempi brevi e con poco dispendio di energie l'ago, rappresentante l'informazione cercata, negli enormi pagliai messi a disposizione dalle nuove tecnologie della gestione digitale delle informazioni. Per questi motivi, oggi ancora più di ieri, **la Pubblica Amministrazione è investita di un'enorme responsabilità nel gestire in modo sicuro le proprie banche dati sempre più dettagliate e tra esse interattive.** Il Codice dell'amministrazione digitale in più punti sottolinea che il diritto all'uso delle tecnologie informatiche nei rapporti con la pubblica amministrazione e tra pubbliche amministrazioni deve essere improntato e reso operante nel rispetto delle norme di sicurezza e di protezione dei dati personali in modo da garantire l'esattezza, la

disponibilità, l'accessibilità, l'integrità e la riservatezza degli stessi dati.

4. GENESI STORICA DI UN DIRITTO FONDAMENTALE DELL' *"HOMO TECNOLOGICUS"*

Una breve ricostruzione delle origini di un diritto che diviene "fondamentale" in una società che necessita sempre più di dati ed informazioni per poter crescere e per poter offrire maggiore benessere contribuisce a mettere nel quadro dei valori e dei principi a cui l'operato non solo della Pubblica Amministrazione ma anche quella di ogni singola persona si deve ispirare.

Il diritto al rispetto della vita privata trova una delle sue prime concretizzazioni concettuali nell'ordinamento giuridico statunitense celato dietro le rivoluzionarie intuizioni di due brillanti studiosi (WARREN - BRANDEIS). **L'esigenza di proteggere l'elemento psicologico e relazionale della persona**, oltre a quello fisico, fu avvertita come pressante non appena le tecniche fotografiche vennero perfezionate al punto da essere percepite come invasive e potenzialmente pericolose per la propria immagine privata e pubblica. **La riduzione dell'individuo ad un'immagine** impressa su un pezzo di carta riproducibile in numerose copie fedeli all'originale e circolabili senza possibilità alcuna di controllo da parte del soggetto in esso riprodotto, **creò nell'immaginario sensazioni e timori** molto simili a quelli che si avvertono nei confronti delle

nuove tecnologie tese, per loro intima essenza, a catturare un numero enorme di informazioni, testi o immagini, elaborarle e renderle disponibili sulla base di una semplice richiesta. La similitudine è data dal fatto che attraverso le nuove tecnologie della gestione delle informazioni un complesso di dati di rilevanza personale fornito o catturato, in un determinato momento e per un determinato fine, riesce a raffigurare e delineare il profilo di un individuo, fissandolo e cristallizzandolo nello spazio e nel tempo come in una fotografia e in modo avulso dalle condizioni originarie, di cui quei dati o quelle particolari informazioni costituivano espressione. Ritornando alle origini della *privacy*, la questione non fu affrontata utilizzando i classici canoni dello *ius excludendi* del diritto di proprietà o con il ricorso al concetto del pericolo per l'onore o la reputazione del soggetto coinvolto, ma venne in rilievo qualcosa di più intimo e profondo: la personalità dell'individuo, sintesi di elementi fisici e, ancor di più, di complessi ed imperscrutabili aspetti psicologici. Partendo dalla consapevolezza di dover solcare nuove strade, la Corte Suprema statunitense elaborò così una cospicua giurisprudenza mettendo in evidenza, scolpendone le varie sfaccettature, i numerosi aspetti in cui si concretizzava la brillante intuizione degli autori precedentemente citati (GERMANI; BALDASSARE; RODOTÀ). Le due facce della medaglia su cui si mossero giudici e

studiosi, scivolando da un caso all'altro, erano costituite: dall'esigenza di erigere un muro, un confine invalicabile, a protezione del singolo e delle sue informazioni personali che non potesse essere oltrepassato senza il consenso esplicito del singolo individuo (**aspetto passivo**); la libertà di poter compiere scelte personali ed intime in piena autonomia e senza il pericolo di essere influenzato dalle critiche o dalla disapprovazione dell'ambiente circostante (**aspetto attivo**). In Europa le cose andarono in modo diverso, tranne che in qualche rara eccezione, infatti, gli Stati del Vecchio continente non elaborarono un istituto analogo alla *privacy* statunitense. La frammentarietà divenne la caratteristica principale di una cultura giuridica disposta ad affrontare i problemi che questa materia poneva con intensità crescente, sempre solo come enigmi da risolvere non seguendo una logica d'insieme e curandosi esclusivamente di trovare, talvolta slabbrando le fattispecie normative, una soluzione utile solo per il singolo caso, piuttosto che cercando di costruire archetipi generali da cui trarre in modo deduttivo la soluzione del caso concreto. La fine di questa frammentarietà si può simbolicamente far risalire all'art. 8 della Convenzione europea per i diritti dell'uomo e delle libertà fondamentali (d'ora in poi CEDU) e all'interpretazione che di esso ha fatto la Corte di Strasburgo: «1. Ogni persona ha il diritto al

rispetto della vita privata e familiare, del suo domicilio e della sua corrispondenza. 2. Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del Paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui.».

La Corte di Strasburgo, sulla falsariga tracciata dalla Corte Suprema statunitense, costruì con la sua giurisprudenza due binari su cui far scorrere la disciplina del diritto alla riservatezza: il primo attento a punire l'abuso delle informazioni personali tese a creare un profilo dell'utente al fine di evitare situazioni potenzialmente pericolose; il secondo, più ampio e difficilmente rinchiudibile nell'angusto limite di una definizione, teso a porre delle garanzie affinché ogni individuo fosse schermato dal pericolo di "sguardi indiscreti" limitativi della propria autonomia. L'importanza della CEDU e la forza argomentativa della giurisprudenza della Corte di Strasburgo vennero sottolineate dalle ripercussioni che queste provocarono sulle strutture normative dei singoli Stati europei e su quelle comunitarie. Questa "bomba di profondità", filtrando e scorrendo lentamente attraverso le acque di ordinamenti giuridici frutto di secolari sedimentazioni culturali,

raggiunse la mente dei popoli europei collocandosi accanto ad istituti giuridici di antica tradizione; infine, dopo essersi ritagliata una propria identità, inevitabilmente scoppiò creando delle onde d'urto che difficilmente vennero contenute dai tradizionali strumenti giuridici. Nel diritto comunitario, in origine, non era presente una scacchiera di diritti umani riconosciuti all'interno degli statuti istitutivi (MANCINI). Sarà la Corte di Giustizia della Comunità europea con un'imponente opera giurisprudenziale a riconoscere, in un primo tempo, i diritti fondamentali della persona inserendoli all'interno di quei principi che essa stessa aveva il compito di garantire. Le premesse logiche di queste pronunce si ritrovano in quella giurisprudenza della Corte di Strasburgo precedentemente indicata e nelle tradizioni costituzionali degli Stati membri più sensibili al problema della tutela e della promozione dei diritti fondamentali. Tali basi costituiranno l' "humus" idoneo a far germogliare i diritti dell'uomo nella coscienza europea e condurranno, successivamente, alla redazione dell'art. 6 TUE e alla solenne proclamazione della Carta dei diritti fondamentali dell'Unione europea nel Consiglio europeo svoltosi il 7 dicembre 2000 a Nizza. Per questo motivo appare necessario premettere ad ogni discorso in tema di diritto alla riservatezza e di tutela dei dati personali, sia a livello nazionale che internazionale, le conclusioni

raggiunte in sede di interpretazione giurisprudenziale della CEDU. La Corte europea per i diritti dell'uomo è stata investita più volte del problema della violazione della "vita privata" ex art. 8 CEDU in relazione a presunti abusi dell'utilizzazione di informazioni personali. Come si evince dalla lettura della norma, l'ambito di operatività dell'articolo predetto non appare limitata a determinate e specifiche ipotesi; tuttavia, «non ci sembra però essere priva di limiti, e in particolare crediamo si possa affermare che l'oggetto della protezione è la sfera personale, privata, in qualche modo psicologica dell'individuo. Ne fuoriesce quell'attività esclusivamente sociale e intimamente legata all'agire collettivo, come tale di non esclusiva pertinenza del singolo» (PALLARO). L'ambito della non ingerenza nella "vita personale", per quanto ampiamente interpretato, non si spinge mai oltre il confine del lecito, sino al punto da poter coprire eventuali attività illegali. Un'altra questione sorge proprio in considerazione del carattere personale di questo diritto fondamentale: le persone giuridiche possono essere considerate titolari di un diritto così "personale"? Nonostante in dottrina le opinioni non siano concordanti, «sinora, per lo meno, la Corte di Strasburgo non lo ha mai riconosciuto; in tutte le occasioni in cui ha accolto entro il raggio d'azione l'art. 8 comunicazioni o ambienti professionali e commerciali, lo ha fatto sempre in

riferimento a persone fisiche e con argomenti che ci sembrano calzare solo su di esse» (PALLARO). Le esigenze legate all'espletamento delle indagini penali e della prevenzione del crimine, spesso, si scontrano con i contenuti dell'art. 8 CEDU creando dei momenti di frizione, difficilmente risolvibili sempre a favore del singolo individuo. Accanto a questa congerie di situazioni riconducibili al contenuto dell'art. 8 CEDU, si affianca ed emerge con forza il diritto a conoscere, entrare in possesso ed eventualmente modificare le informazioni personali da altri custodite. La persona ha il diritto di ritagliare il suo profilo e sovrapporlo a quello che altri hanno ricostruito tramite il reperimento e l'elaborazione di informazioni relative alla sua persona, intesa come identità biologica e di utente-consumatore. Il segreto professionale assume un valore importante, totalizzante, per l'instaurazione e il mantenimento del rapporto di fiducia medico/paziente; per questo motivo, la Corte impone che il segreto venga garantito, anche dopo la cessazione del servizio, non solo per il personale medico che entra in diretto contatto con il malato, ma anche per tutti gli operatori che si trovano a lavorare e trattare dati così particolari e sensibili. La giurisprudenza della Corte di Strasburgo sembra, in estrema sintesi, aver costruito le motivazioni delle sue decisioni sul fondamento che le informazioni personali siano realtà proprie di ciascun individuo.

Di conseguenza la loro disponibilità è strettamente legata alla volontà del titolare che ha il diritto di determinare in modo autonomo le proprie azioni e i propri pensieri ed, inoltre, impedire che dalle informazioni personali reperibili si possa ricostruire un profilo per lui ingiustamente penalizzante. Se quello appena descritto è rivelatore di un fondamentale diritto dell'uomo degno di massima tutela, dall'altra parte non si deve incorrere nell'errore di considerarlo in una prospettiva assoluta e senza possibilità alcuna di attenuazione. «Ebbene, in quanto ciascuno è membro della società in cui vive, sarebbe inimmaginabile concedergli un dominio assoluto su ogni notizia a sé riferita. Da questa concezione della persona umana seguono: l'ammissibilità, entro certi limiti chiari in partenza e ragionevoli, di molti e svariati utilizzi di dati personali; l'inammissibilità di pretese di una sorta di esclusiva su informazioni inerenti a proprie attività specificamente rivolte alla generalità, o su dati personali comunque attinenti a contesti sociali non inscindibilmente legati all'esperienza personale del singolo» (PALLARO). La moderna società è costituita da una fitta rete di rapporti e relazioni interpersonali reali e/o virtuali in cui l'elemento base è l'informazione. Flussi continui di dati scorrono lungo le vie telematiche senza trovare mai sosta, rendendo nulla la rilevanza di ogni distanza fisica tra i soggetti coinvolti. Tra le

innumerevoli categorie di informazioni quelle che rivestono un ruolo particolarmente degno di attenzione e di tutela contro pericoli di abusi sono quelle personali, riferite cioè a persone ben determinate o determinabili. Il pericolo sempre pronto a concretizzarsi, in una società moderna nelle strutture ma ancora largamente vetusta nella cultura, è l'utilizzo di tali informazioni in chiave discriminatoria e al fine di creare profili personali per scopi ignorati dall'utente e, nei casi più gravi, illeciti. Quello che nasce e prende corpo in Europa, grazie alla CEDU e alla giurisprudenza della Corte di Strasburgo, è la coscienza di un diritto fondamentale al dominio sulle proprie informazioni personali ed al diritto esclusivo di costruire la propria identità personale (PAGANELLI; SANTANIELLO; LOIODICE) «La posizione giuridica che entra in gioco, complessivamente, può definirsi “diritto di autodeterminazione sulle proprie informazioni”, o più concisamente, come è stato proposto, “autodeterminazione informativa” od “informatica” (PALLARO).

5. DALLA CONVENZIONE DI STRASBURGO AL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Ripercorrendo sinteticamente l'*iter* che ha preceduto l'entrata in vigore della prima legge italiana dedicata in modo precipuo alla tutela dei dati personali, la legge 675/96, è necessario soffermarsi brevemente sul contesto europeo che ne rappresentò la premessa logica e culturale.

La Convenzione “sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale” è stata ratificata e resa esecutiva dalla legge 21 febbraio 1989, n. 98 (G.U. n. 66 del 20 marzo 1989). Lo strumento con cui la Convenzione è stata introdotta nel nostro ordinamento giuridico statale è denominato “ordine d'esecuzione”. Il contenuto del trattato a causa della natura *non-self executing*, desumibile chiaramente dall'art. 4 e dal tenore delle altre disposizioni, subordina la sua efficacia all'adozione di apposite norme interne che ne rendano operativo il contenuto all'interno dell'ordinamento degli Stati (Parti). La Convenzione tenta di mediare e di trovare un difficile equilibrio tra due opposte esigenze: la libertà della circolazione delle informazioni e i diritti fondamentali della persona. L'oggetto del Trattato è individuato e delimitato dall'art. 1: «Scopo della presente convenzione è quello di garantire, sul territorio di ogni Parte, ad ogni

persona fisica, qualunque siano la sua cittadinanza o residenza, il rispetto dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata, nei confronti dell'elaborazione automatizzata dei dati di carattere personale che la riguardano («protezione dei dati»)). L'oggetto di protezione è individuato in ogni informazione relativa alla persona che, inserita in uno schedario informatico, diventi possibile oggetto di "elaborazione automatica". L'altro elemento discriminante, ai fini dell'applicabilità della normativa in esame, è l'identificazione del responsabile di tale schedario «con la persona fisica o giuridica, l'autorità pubblica, l'ente o altro organismo competente, secondo il diritto nazionale, a decidere quale debba essere la finalità del casellario automatizzato, quali categorie di dati a carattere personale debbano essere registrati e quali operazioni siano ad essi applicabili». E', in altre parole, la "qualità" dei dati (a carattere personale) e il "tipo" del mezzo utilizzato (elaborazione automatizzata) a disegnare il perimetro all'interno del quale opera detta disciplina. In merito alla suddetta "qualità dei dati" e alla loro elaborazione i principi fissati dalla Convenzione sono così sintetizzabili: 1. **la liceità e la correttezza** (principio di lealtà e buona fede) del reperimento e dell'elaborazione automatica dei dati; 2. **la legittimità** (principio di legalità) e la determinazione anticipata dei fini, motivo e causa della registrazione; 3. **l'impiego dei dati**

reperiti ed elaborati in stretta conformità con i fini predetti; 4. **l'adeguatezza dell'uso al fine**, intesa come sufficiente e non eccessiva utilizzazione dei dati oltre il minimo necessario per il raggiungimento dello scopo; 5. **la correttezza dei dati e il loro possibile aggiornamento** (da parte degli interessati) nel caso in cui si rivelassero errati o semplicemente “non più corrispondenti alla realtà”; 6. **i dati devono essere conservati in modo da risalire alle persone interessate, per un tempo che non ecceda quello sufficiente a raggiungere i fini per i quali sono stati registrati ed elaborati.** Accanto a questi principi di carattere generale, operanti per l'intera categoria “dati di rilevanza personale”, la Convenzione detta una particolare, e più rigida, disciplina per alcuni tipi di dati personali ritenuti particolarmente “sensibili”, la cui schedatura è ritenuta potenzialmente rischiosa. All'interno di questa tipologia di dati sono collocati quelli indicanti: l'origine razziale, le opinioni politiche, le convinzioni religiose, i dati relativi allo stato di salute e alla vita sessuale ed infine, quelli relativi alle condanne penali. A causa della pericolosità intrinseca ad elaborazioni automatiche aventi ad oggetto questo tipo di dati, la Convenzione detta una norma generale che vieta tali operazioni a «meno che il diritto interno non preveda garanzie adatte». La scelta di un'elencazione così dettagliata della fenomenologia dei dati c.d. “sensibili” non è vista in modo

favorevole da una parte della dottrina che intravede, in tale tecnica, una inutile limitazione e costrizione dell'oggetto di tutela che potrebbe provocare futuri dubbi interpretativi e vuoti di difesa (WACKS; LATTANZI). Tuttavia, al legislatore della convenzione può essere mossa la critica di non avere sufficientemente specificato agli Stati, Parti del trattato, gli strumenti e i livelli minimi idonei a garantire la necessaria vigilanza e difesa di questi particolari dati personali. Un punto di fondamentale importanza è rappresentato dal contenuto dell'articolo 8, «Ulteriori garanzie per la persona interessata», delineante una serie di poteri che ogni individuo può esercitare nei confronti di un casellario automatizzato e del suo responsabile. Innanzitutto, ogni persona deve poter conoscere: l'esistenza di un casellario automatizzato di dati a carattere personale e gli scopi per i quali è nato; l'identità, la residenza abituale e la sede amministrativa del suo responsabile. Inoltre, deve poter conoscere, senza incontrare eccessive difficoltà e costi elevati, l'esistenza all'interno di tali archivi di dati ad esso relativi e, in caso affermativo, poterne estrarre copia al fine di verificarne la veridicità e la liceità. Nel caso in cui si riscontri un errore si deve poterne ottenere la rettifica o l'aggiornamento od eventualmente, in caso di illegalità del trattamento, la cancellazione. Tutte queste disposizioni sarebbero risultate vane, al fine di una concreta tutela, senza la

previsione contenuta nella lett. d) dell'art. 8 che impone agli Stati di disporre gli interventi necessari a rendere effettiva una «... possibilità di ricorso qualora non venga dato seguito ad una richiesta di conferma o, a seconda del caso, di comunicazione, rettifica, o cancellazione» relativa alle richieste precedentemente illustrate. Uno dei motivi di fondo dell'intera disciplina è individuabile nell'indirizzo teleologicamente imposto, come imprescindibile elemento, al reperimento e all'elaborazione dei dati personali; l'idea del "fine", infatti, segna e scandisce tutte le fasi della vita di quello che la Convenzione definisce casellario di dati. Si deve aggiungere che l'obbligo imposto di "responsabilizzare" i "responsabili" dei casellari suddetti non è assoluto, ma prevede significative, e a volte troppo estese, deroghe che consentono agli Stati di mitigare la rigidità di detta disciplina. Il parametro utilizzato per consentire queste limitazioni del diritto all'autodeterminazione informativa è quello «della necessità in una società democratica...»; questa formula si riallaccia a quella dell'art. 8 CEDU e alla copiosa giurisprudenza di Strasburgo in materia. Una volta fissati, negli articoli precedentemente commentati, gli estremi della tutela, la Convenzione affronta la spinosa questione del flusso di dati di rilevanza personale oltre frontiera. Si tenta così, dopo aver inclinato il piano della bilancia ponendo sul piatto dei diritti fondamentali

numerosi pesi, di riequilibrarlo collocando sull'altro, quello dedicato alla libertà di circolazione delle informazioni, il principio per cui: «una Parte non può, ai soli fini della protezione della vita privata, proibire o condizionare ad una autorizzazione speciale il movimento oltre frontiera di dati a carattere personale destinati al territorio di un'altra Parte» (art. 12, n. 2). Anche in questo caso all'enunciazione del principio seguono numerose possibilità di deroghe; ma l'aspetto che più di altri è importante, in questa sede, sottolineare, perché possibile oggetto di critica, è la mancanza di una specifica previsione di restrizioni al trasferimento di dati personali verso i paesi non contraenti. Tuttavia, in questa materia è intervenuta con decisione la normativa comunitaria che ha dedicato maggiore attenzione alla disciplina del movimento transfrontaliero dei dati personali verso Paesi extracomunitari colmando così la lamentata lacuna. La Convenzione di Strasburgo del 1981 n. 108 continua ancora oggi, ad anni di distanza dalla sua formulazione, a rappresentare un testo di fondamentale importanza per chiunque voglia conoscere le origini, giuridiche e storiche, del diritto all'autodeterminazione informativa ed acquisire una sensibilità e un metodo utile ad affrontare lo studio di una materia così vasta e caratterizzata dalla frammentarietà dei suoi contenuti. La grandezza della Convenzione, nonostante la formulazione ampia delle sue fattispecie e la presenza di deroghe che

sembrano vanificare il contenuto di alcuni principi, risiede in quel piccolo, ma allo stesso tempo rilevante, nucleo fondamentale ed irrinunciabile di garanzie imposte agli Stati che nel tempo è riuscito a promuovere ed ottenere un avvicinamento ed una armonizzazione delle diverse discipline nazionali. Per concludere, parlando del rapporto tra la libertà della circolazione delle informazioni e i diritti fondamentali non si può far finta di nulla e tralasciare di considerare, anche se brevemente e solo ponendo le basi della questione, i possibili effetti che su di esso hanno prodotto i terribili e noti attentati terroristici che hanno colpito, con gli Stati Uniti d'America, tutto il mondo innescando delle terrificanti reazioni a catena che si ripercuotono, ormai quotidianamente, sulla sfera della vita privata di ogni individuo. La riflessione che si vuole compiere parte dalla constatazione che fino a qualche anno addietro la gran parte della popolazione europea era pronta a condannare e stigmatizzare, come strumenti propri di uno "Stato Autoritario e di Polizia", operazioni compiute su larga scala tese alla raccolta indiscriminata di masse di dati (in particolare di rilevanza personale) per fini di prevenzione del crimine, perché avvertite come invasive della sfera più intima e personale di ciascuno. Oggi, alla luce di questi terribili eventi, un angoscioso quesito si pone all'attenzione dei nostri "governanti": si può affermare pacificamente che le considerazioni predette siano

rimaste immutate e che la società europea sia disposta a non retrocedere sulla soglia dei traguardi raggiunti in tema di autodeterminazione informativa, sacrificandoli sull'altare di un rafforzato "bisogno pubblico" di sicurezza teso ad incrementare l'intensità dei controlli e delle "schede personali" per fini di prevenzione di crimini così crudeli e disumani ? Quello che si può aggiungere è un invito ad ancorarsi a quei minimi valori comuni in tema di trattamento dei dati di rilevanza personale e cercare, anche in un periodo storico così difficile, di non cedere alla facile tentazione di sconvolgere la gerarchia dei valori portanti della nostra moderna e liberale società, giustificando ogni ingerenza nella vita privata del singolo individuo con il semplice e vuoto richiamo ad una esigenza di sicurezza pubblica. Per non perdere conquiste culturali così importanti che ancora una volta, e nonostante tutto, bisogna cercare caso per caso il "giusto mezzo" tra la sicurezza, nella sua dimensione pubblica, e la *privacy*, nella sua dimensione individuale e personale, non accontentandosi mai di aprioristiche ed immotivate scelte di controlli indiscriminati di massa.

A seguito della convenzione di Strasburgo, l'Europa dedicò notevoli risorse al raggiungimento di un migliore ed uniforme livello di protezione nella circolazione e nel trattamento automatizzato dei dati e delle informazioni. In tale ottica venne adottata la Direttiva

95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, recante “tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati” con l’espreso obiettivo di individuare standard di protezione validi ed uniformi a livello europeo (MINELLA). I principi sanciti dalla Convenzione di Strasburgo furono precisati e sviluppati nella citata direttiva tesa ad rimuovere il divario nei livelli di tutela dei diritti e delle libertà personali garantiti negli Stati membri relativamente al trattamento di dati personali. L’ordinamento giuridico italiano attuò tale Direttiva attraverso la promulgazione della **legge 31 dicembre 1996 n. 675**, “Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali”. In base a quanto indicato nella legge 675/1996 ogni trattamento dei dati personali deve svolgersi nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone, con particolare riferimento alla riservatezza e all’identità personale in modo da ridurre al minimo, mediante l’adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Recentemente la disciplina italiana relativa al trattamento dei dati personali è stata riscritta dal legislatore nel **Decreto Legislativo 30**

giugno 2003 n. 196 “Codice in materia di protezione dei dati personali”, entrato in vigore il 1° gennaio 2004. Tale fonte raccoglie ed organizza organicamente la precedente normativa relativa al trattamento dei dati personali, divenendo così il testo di riferimento in materia di tutela dei dati personali.

Il Codice in materia di protezione dei dati personali si compone di 186 articoli ed si suddivide in tre parti: la prima è dedicata alle disposizioni generali e definisce tutti gli adempimenti e le regole da osservare nel trattamento dei dati personali nel settore pubblico e privato; la seconda tratta specifici settori: trattamenti nei settori giudiziario, pubblico e sanitario, negli ambiti di lavoro, nel sistema bancario, finanziario ed assicurativo; la terza reca le disposizioni in materia di tutela dell'interessato e di sanzioni, oltre alle disposizioni sull'Ufficio del Garante.

6. IL TRATTAMENTO DEI DATI PERSONALI NELLA PUBBLICA AMMINISTRAZIONE: I PRINCIPI GENERALI

La disciplina del Codice si innesta in un contesto orientato verso la trasparenza e la pubblicità dell'azione amministrativa. **L'azione amministrativa deve essere, quindi, ispirata alla protezione dei dati personali quale prerogativa fondamentale della persona.** Tale diritto deve considerarsi autonomo e distinto dal diritto alla riservatezza in quanto diretto ad attribuire al suo titolare il diritto pieno ed assoluto di conoscere e controllare la circolazione delle informazioni che lo riguardano. L'obiettivo del legislatore è quello di garantire che il trattamento dei dati personali avvenga nel pieno 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 (art. 2 del Codice). Una delle regole fondamentali che deve essere sempre tenuta in considerazione dalla Pubblica Amministrazione è quella relativa alla **necessità di trattare i dati personali osservando i principi di pertinenza e non eccedenza dei dati trattati.** Per adempiere alla suddetta regola, la Pubblica Amministrazione deve, ad esempio, impiegare strutture hardware e software in modo da utilizzare al minimo i dati personali escludendone il trattamento quando le finalità perseguite possono

essere raggiunte mediante l'uso di dati anonimi o di modalità che permettano di identificare l'interessato solo in caso di necessità (art. 3 del Codice). Il principio di necessità costituisce un presupposto di liceità del trattamento dei dati personali ed il mancato rispetto di questo e degli altri principi comporta conseguenze giuridicamente rilevanti. Infatti, il Codice, nel dettare le regole per tutti i trattamenti ha sancito l'inutilizzabilità dei dati personali trattati in violazione della disciplina in materia di trattamento dei dati personali (art. 11, secondo comma, del Codice).

La disciplina in esame, si permea di proprie sfumature semantiche nel momento in cui le norme vengono lette nella prospettiva che lega la persona allo Stato ed alle sue innumerevoli diramazioni funzionali e strumentali. L'articolo 1 del Codice riconosce a "chiunque" il diritto alla protezione dei dati personali che lo riguardano. Il legislatore non compie alcuna distinzione soggettiva in merito alla titolarità del predetto diritto che spetta a "chiunque" sia esso cittadino, straniero, persona fisica o giuridica (LISI – BERTONI). Nella predetta ottica, la Pubblica Amministrazione ha l'obbligo di garantire la protezione dei dati personali in suo possesso ed acquisiti per poter adempiere agli scopi istituzionali a cui è preposta. Nel momento in cui il legislatore sancisce tale diritto, ampio ed incondizionato, la Pubblica Amministrazione deve predisporre

quanto necessario per operare in un regime di legalità senza violare il contenuto di tale normativa.

*Il Codice in materia di protezione dei dati personali (d.lgs.196/03) riconosce al titolare del diritto il ruolo di unico "sovrano" delle informazioni che lo riguardano (Giudice di pace, sez. III, Napoli, 26.6.04, n. 8432 in *Il merito*, 2004, 9, 19).*

Sin da queste premesse si desume chiaramente che per soddisfare il diritto alla protezione dei dati personali la Pubblica Amministrazione deve attivarsi predisponendo le risorse e le competenze necessarie per soddisfare quanto imposto dalla legge. Si tratta, quindi, di intervenire profondamente sia a livello procedurale e strumentale e sia a livello formativo e culturale. In altre parole, la protezione dei dati personali impone alla Pubblica Amministrazione di attivarsi per attuare la legge e non di subire passivamente la suddetta normativa. E' connaturata allo stesso concetto di sicurezza l'esigenza di una dinamicità intrinseca del sistema oggetto di tutela.

L'agire della Pubblica Amministrazione, nell'ambito del trattamento dei dati personali, si deve realizzare 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 legislatore richiede una particolare attenzione ai soggetti che trattano dati personali imponendo ad essi un controllo sull'operazione o complesso di operazioni, effettuate 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 dei dati personali non può essere più considerato come un'attività di routine da parte della Pubblica amministrazione, in generale, e dei dipendenti pubblici, in particolare. E' necessario prendere coscienza che i dati personali acquisiti sono un bene da tutelare e proteggere perché afferenti ad una persona, fisica o giuridica, e che un eventuale trattamento illecito e/o non sicuro degli stessi potrebbe arrecare una grave offesa ai diritti ed alle libertà fondamentali del soggetto interessato. Un trattamento dei dati personali non conforme alla legge potrebbe ledere, oltre al predetto diritto alla protezione dei dati personali, i diritti costituzionalmente riconosciuti alla dignità, alla riservatezza ed all'identità personale del soggetto interessato. Il secondo comma dell'art. 2 del Codice detta il c.d. "principio di semplificazione nell'elevata tutela" (DI MARTINO – VOLTAN) in base al quale una tutela

elevata dei dati personali deve essere garantita nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento. L'importanza di questo principio risiede nella consapevolezza, da parte del legislatore, che per la concreta realizzazione di un diritto nella prassi quotidiana è necessario creare procedure ed automatismi amministrativi idonei a semplificare ed armonizzare le modalità di realizzazione dello stesso, sia a vantaggio dell'interessato e sia a favore del titolare del trattamento. Alla luce della sempre crescente informatizzazione della Pubblica Amministrazione assume rilievo il principio di necessità nel trattamento sancito dall'art. 3 del Codice per cui i sistemi informativi e i software devono essere configurati sin dall'origine riducendo al minimo l'utilizzazione di dati personali e di dati identificativi. L'attuazione di tale principio comporta l'esclusione del trattamento dei suddetti dati quando le finalità perseguite nei procedimenti possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Si desume chiaramente da quanto contenuto nell'art. 3 del Codice un *favor* del legislatore per l'utilizzo dell'anonimato nei sistemi informativi e nei software (LISI – BERTONI).

In merito all'ambito di applicazione della normativa in esame, il legislatore puntualizza che trova vigenza la disciplina del Codice nel caso di trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello stesso. Il Codice recepisce così, nell'ambito del trattamento dei dati personali, il principio di derivazione comunitaria c.d. di “stabilimento” ossia il criterio di collegamento in base al quale l'applicazione del Codice dipende dal fatto che il soggetto che tratta i dati sia stabilito nel territorio dello Stato o in un luogo soggetto alla sua sovranità (DI MARTINO – VOLTAN). Inoltre, tale normativa si applica anche alle ipotesi di trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici. In caso di applicazione del Codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali. Tuttavia, il Codice non trova applicazione nell'ipotesi in cui il

trattamento di dati personali venga effettuato da un soggetto stabilito nel territorio di un Paese non appartenente all'Unione europea sebbene utilizzi degli strumenti situati nel territorio dello Stato quando questi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea.

Di particolare interesse è l'ultimo comma dell'art. 5 del Codice in cui si afferma che il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del Codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione.

La Corte di Cassazione afferma in una recente sentenza che:

«L'art. 5, terzo comma, infatti, prevede che il trattamento (e quindi la comunicazione) di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione delle disposizioni di cui al testo unico, solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione, ferma restando peraltro la applicazione delle disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 1 e 31. Pertanto, quando si tratta di persona fisica che effettua il trattamento per fini esclusivamente personali, il soggetto è tenuto a rispettare le disposizioni del testo unico, ivi comprese quelle in tema di obbligo di consenso espresso dell'interessato per il trattamento e quelle in tema di obbligo di notificazione, solo quando i dati raccolti e trattati sono destinati alla comunicazione sistematica ed alla diffusione». Nella

fattispecie «...i dati in questione sarebbero stati forniti dall'imputato a quattro provider al fine di aprire un sito internet e tre nuovi indirizzi di posta elettronica, e quindi in realtà, sempre secondo il capo di imputazione, non sarebbero stati esposti alla pubblica consultazione, ma solo consegnati ad un imprenditore privato fornitore del servizio richiesto, sicché non può configurarsi una diffusione di dati o una comunicazione sistematica, non essendovi un pubblico accesso agli stessi o una loro immediata esposizione. Non può quindi ritenersi che l'imputato, in relazione al trattamento dei dati de quibus, fosse soggetto agli obblighi stabiliti dal d.lgs. 30 giugno 2003, n. 196....Ora, come si è dianzi osservato, nel caso in esame la comunicazione è stata effettuata da una persona fisica per fini esclusivamente personali e riguardava dati non destinati ad una comunicazione sistematica o alla diffusione, e pertanto, ai sensi dell'art. 5, terzo comma, non trovavano applicazione le disposizioni di cui al d.lgs. 30 giugno 2003, n. 196». (Cass. pen., sez. III, 15.2.05, n. 5728 in CED RV230834)

Anche nel caso in cui il trattamento di dati personali venga effettuato da persone fisiche per fini esclusivamente personali si dovranno comunque applicare le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31 della stessa normativa.

7. DEFINIZIONE DI DATI PERSONALI, SENSIBILI, GIUDIZIARI ... E BIOMETRICI

Il Codice dedica ampio spazio alle definizioni, creando un ottimo ausilio per l'interprete che può così rifarsi ad esse per limitare o ampliare il campo di applicazione delle disposizioni di volta in volta esaminate. In primo luogo, quindi, è necessario soffermarsi su quanto puntualizzato dal Codice (art. 4) in merito alla fenomenologia del dato personale:

1. il **"dato personale"** è qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

In ordine alla definizione di "dato personale" è utile leggere un passo di una sentenza della Corte di Cassazione:

Si tratta di stabilire se la legge n. 675 si riferisca (e sia applicabile), o meno, a dati o notizie pubbliche, ovvero il suo ambito sia ristretto alle sole informazioni e notizie private, personali, non usualmente a disposizione di chiunque. L'art. 1 della legge riferisce la tutela, particolarmente "alla riservatezza e all'identità personale", ossia alla salvaguardia di notizie che non siano già conosciute o usualmente conoscibili dal pubblico o da un

vasto pubblico di persone. Né la situazione è sostanzialmente mutata a seguito dell'entrata in vigore del D.Lgs n. 196 del 2003, il quale ha esteso tale riferimento anche al "diritto alla protezione dei dati personali", poiché tale figura giuridica soggettiva presuppone che sia già chiarita la nozione di "dato personale", che è - propriamente - il punto di partenza. Né, sotto questo profilo, soccorre molto la definizione contenuta nell'art. 1, comma 2, lett. c), della legge n. 675 (e, ora, l'art. 4, comma 1, lett. b), D. Lgs. n. 196), la quale riferisce tale nozione a "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione ... anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale". In realtà, qualcosa di più concreto emerge dall'estensione della disciplina stabilita dalla legge 675, dapprima, e dal d.lgs. n. 196, poi, dall'esame della quale si comprende che l'oggetto "immateriale" della tutela (se così può definirsi la impalpabile realtà che forma il dato personale, il quale viene esteso fino alle cd. tracce elettroniche) va ben oltre i dati e le notizie di natura privata e attinge anche ai dati già pubblici o pubblicati, poiché si ritiene che colui che compia operazioni di trattamento di tale informazioni, dal loro semplice accostamento, comparazione, esame, analisi, congiunzione, rapporto, incrocio, ecc., possa ricavare ulteriori informazioni che si rivelino, perciò stesso, un "valore aggiunto informativo", un quid pluris non ricavabile dalle singole unità isolatamente considerate, ma potenzialmente lesivo della dignità dell'interessato (art. 3, primo comma, prima parte, e art. 2 Cost.), valore sommo (anche presente nelle Carte sovranazionali, variamente efficaci anche nell'ordinamento interno) alla cui tutela è ispirata la legislazione

sul trattamento dei dati personali. Di qui la minuta disciplina amministrativa sull'attività di trattamento dei dati, le sue limitazioni, le sue eccezioni, gli strumenti di tutela posti a presidio dei beni protetti, e innanzitutto, dei diritti della persona, ma anche quelli previsti in favore degli "operatori" del trattamento, portatori di altri interessi (di natura storiografica, scientifica, sociologica, giornalistica, ecc.) variamente tutelati.

(Cass. civ., sez. I, 25.6.04, n. 11864)

2. i "**dati identificativi**" sono i dati personali che permettono l'identificazione diretta dell'interessato;

3. i "**dati sensibili**" sono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

In merito alla definizione di dati sensibili si riporta quanto affermato dal Consiglio di Stato in una recente pronuncia:

...quanto il concetto di "dati sensibili" è precisato dall'art. 22 L. 31.12.1996 n. 675 (ribadito dall'art. 4 D. L. vo 30.6.2003 n. 196), in base al quale sono tali "i dati personali idonei a rivelare l'origine razziale od

etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati od associazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale" e tra di essi non rientrano i dati relativi alla professione ed al domicilio di una persona.

(Cons. Stato, sez. V, 11.5.04, n. 2966)

4. i "**dati giudiziari**" sono i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60e 61 del Codice di procedura penale.;

5. il "**dato anonimo**" è il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

6. i "**dati biometrici**" che in questi ultimi mesi sono stati oggetto di alcuni provvedimenti del Garante per la protezione dei dati personali che vanno ad integrare e in alcuni casi ad esplicitare la disciplina in materia. Il Garante in precedenza si era occupato di biometria analizzando in modo specifico l'impiego di rilevatori di impronte digitali per l'accesso nella banche senza giungere però ad

una visione organica del problema. In definitiva, il Garante aveva acconsentito all'utilizzo di tali sistemi di rilevazione in associazione alla memorizzazione delle immagini. Tale consenso, però, era giustificabile esclusivamente da una previa valutazione in concreto dei rischi compiuta non solo dalle banche ma anche e soprattutto dalle autorità di pubblica sicurezza. Con l'approvazione del provvedimento generale sulla videosorveglianza il Garante è ritornato sulla questione sottolineando che l'utilizzo congiunto di sistemi biometrici e videosorveglianza è lecita solo se subordinata a specifiche e rigorose valutazioni che devono comunque essere sottoposte alla verifica preliminare dello stesso Autorità di controllo. Nel frattempo, l'inserimento dei sistemi di rilevazione biometrici negli istituti bancari era andata avanti anche grazie alla firma, a livello delle prefetture, dei protocolli di intesa per la prevenzione della criminalità promossi dall'ABI. La proliferazione di tali sistemi di identificazione ha causato una notevole preoccupazione da parte dell'opinione pubblica e delle stesse istituzioni statali ed europee. In particolare, le autorità coinvolte si sono rese conto che l'utilizzo dei dati biometrici per l'identificazione dei soggetti autorizzati ad accedere a banche dati riservate (ad esempio archivi contenenti dati sensibili) ha creato dei nuovi e pericolosi archivi di dati ancora più "sensibili". Sulla base di tali motivazioni, il Garante per la

protezione dei dati personali ha analizzato nel dettaglio la questione giungendo a tracciare dei vincoli a tali attività di raccolta.

8. L'ORGANIGRAMMA "PRIVACY": DEFINIZIONI, RESPONSABILITÀ E DELEGA DI FUNZIONI

A questo punto della trattazione è opportuno soffermarsi sulle definizioni relative ai soggetti che sono coinvolti nel trattamento dei dati personali e sui rapporti formali e funzionali tra loro intercorrenti.

L'applicazione della normativa sulla protezione dei dati personali non può prescindere dall'individuazione dei soggetti coinvolti nel trattamento e dai ruoli da questi ultimi svolti nell'ambito del trattamento e dei flussi di informazione che lo stesso determina (DI MARTINO – VOLTAN; IMPERIALI). E' definito "**titolare**" la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, il titolare del trattamento è identificato nell'entità nel suo complesso o nell'unità od organismo periferico che esercita un potere decisionale autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della

sicurezza (art. 28 del Codice). L'autonomia del potere decisionale sulle finalità e modalità del trattamento diviene l'elemento decisivo per l'individuazione, anche in una struttura complessa ed articolata, della figura del titolare.

Nell'ambito dell'organico "privacy" riveste un ruolo di notevole valore strategico la figura del **responsabile**" ossia la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali. Il responsabile ai sensi dell'art. 29 del Codice è una figura eventuale in quanto facoltativamente designato dal titolare. Tuttavia, se quest'ultimo decide di nominarlo ha il dovere di individuarlo tra i soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Le particolari competenze e attitudini tecniche necessarie per svolgere un ruolo di estrema rilevanza e responsabilità impongono così al titolare di compiere una selezione attenta e mirata. E' necessario precisare, inoltre, che per soddisfare delle esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. In tal modo, il titolare si può avvalere dell'ausilio di più soggetti suddividendo tra loro le diverse mansioni. I compiti affidati al responsabile sono

analiticamente specificati per iscritto dal titolare. I responsabili saranno così edotti e vincolati in merito ai compiti da svolgere. Tuttavia, il responsabile non esegue le sue funzioni in piena autonomia ma ha l'obbligo di effettuare il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni sul trattamento dei dati personali e delle proprie istruzioni.

Un ruolo essenziale è svolto dagli "incaricati", ossia dalle persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile ai sensi dell'art. 30 del Codice. Le operazioni di trattamento possono essere effettuate esclusivamente da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. La stessa designazione degli incaricati è effettuata per iscritto individuando puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

Dopo aver esaminato le singole figure coinvolte nel trattamento dei dati si devono compiere, proprio in considerazione delle peculiari caratteristiche strutturali delle amministrazioni pubbliche, alcune riflessioni sul complessivo sistema delle responsabilità in ambito

“privacy”. Da quanto esaminato appare di chiara evidenza come il legislatore abbia voluto dettare le linee di una suddivisione gerarchica delle responsabilità partendo dagli organismi di vertice dell’ente, sia esso pubblico o privato (ERCOLANO). A tali soggetti “apicali” competono, infatti, tutte le decisioni in merito alla predisposizione delle modalità di trattamento e all’adozione delle misure, minime ed idonee, di sicurezza poste a tutela dei dati personali. Come mette ben in evidenza la dottrina più accorta l’impostazione scelta dal legislatore del Codice è strettamente mutuata da quella realizzata nel d.lgs. 626/94 dove i soggetti coinvolti nel processo della sicurezza e della salute dei lavoratori durante il lavoro sono il datore di lavoro, il dirigente e il preposto (art. 4 e ss. d.lgs. 626/94) (ERCOLANO). Ai fini della determinazione, in particolare in ordine alle eventuali responsabilità di tipo penale ed amministrativo, diviene di particolare interesse nell’ambito di strutture di dimensioni rilevanti soffermarsi su quella che può essere definita “**delega di funzioni in ambito privacy**”.

Il titolare, come già affermato in precedenza, ha l’obbligo di attivarsi al fine di adeguare l’attività dell’ente alla disciplina contenuta nel Codice in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle

finalità della raccolta (art. 31 del Codice). E' necessario premettere che nelle ipotesi in cui le realtà aziendali non consentano al titolare di entrare nel merito dell'organizzazione del trattamento dei dati diviene rilevante l'individuazione puntuale del responsabile che da figura normativamente eventuale diviene figura sostanzialmente necessaria. La nomina del responsabile, tuttavia, non esclude un'eventuale responsabilità del titolare poiché spetta sempre a quest'ultimo, ad esempio, vigilare sull'adozione o l'adeguamento delle misure di sicurezza che tengano in considerazione gli standard imposti dalla legge (artt. 33 e 34 del Codice e disciplinare tecnico di cui all'Allegato B); programmare la stesura di un aggiornato Documento programmatico sulla Sicurezza (art. 34); effettuare l'individuazione delle figure coinvolte nel trattamento dei dati (artt. 29 e 30) ed ottemperare agli adempimenti nei confronti del Garante che la normativa pone espressamente in capo a questo soggetto (ad es., notificazione del trattamento). Infine, egli deve comunque operare in base ai criteri generali di diligenza e buona fede, continuando a rispondere sia delle scelte effettuate sia del controllo sull'operato dei soggetti coinvolti nel trattamento (ERCOLANO).

Volendo offrire una chiave di lettura per l'interpretazione delle disposizioni riguardanti la nomina del responsabile in ambito del trattamento dei dati personali si può affermare, mutuando le

conclusioni raggiunte dalla giurisprudenza sulla delega di funzioni nell'ambito del d.lgs. 626/94, che la stessa debba possedere una alcuni imprescindibili requisiti per essere idonea ad escludere un'eventuale responsabilità del titolare: a) le dimensioni della struttura organizzata; b) l'idoneità tecnica del delegato; c) il conferimento effettivo dei poteri; d) l'accettazione da parte del delegato; e) la certezza dell'atto in ordine alla provenienza, al contenuto, alla data della sua formazione (MORRONE).

Sul punto, di estremo interesse appare una recente sentenza della Corte di Cassazione che così descrive le caratteristiche della delega di funzioni nell'ambito del d.lgs. 626/94 (cfr. Cass., Sez. IV, 25.8.2000, 9343; Cass. pen., sez. III 28.7.2000, n. 8585):

...il datore di lavoro è il primo principale destinatario degli obblighi di assicurazione, osservanza e sorveglianza delle misure e dei presidi di prevenzione antinfortunistica contemplate in quel disposto normativo e negli altri che a quello fanno riferimento... Tale precipuo obbligo del datore di lavoro può essere ad altri delegato, ossia trasferito, con conseguente sostituzione e subentro del delegato nella posizione di garanzia che fa originariamente capo al datore di lavoro. Ma, tanto comportando una dismissione da parte del datore di lavoro - specifico e principale, ancorché non esclusivo, destinatario della norma - di tali obblighi assegnatigli dalla legge ed un loro contestuale trasferimento ad

altri, il relativo atto di delega deve essere espresso, non equivoco e certo, dovendo inoltre investire persona tecnicamente capace, dotata delle necessarie cognizioni tecniche e dei relativi poteri decisionali e di intervento, che abbia accettato lo specifico incarico, fermo restando l'obbligo per il datore di lavoro di vigilare e controllare che il delegato usi, poi, concretamente la delega, secondo quanto la legge prescrive
(Cass. pen., sez. III, 15.7.05, n. 26122)

Riprendendo le fila del discorso in materia di delega nell'ambito dell'organico privacy, rileva, anche se non in modo determinante, il fatto che l'ente abbia notevoli dimensioni e si articoli in varie branche. Nel caso di entità di grandi dimensioni, infatti, è più difficile che un soggetto possa eseguire contemporaneamente tutti gli adempimenti previsti dal Codice. L'effettiva capacità ed idoneità professionale e tecnica del responsabile è un requisito richiesto dallo stesso articolo 29, comma 2, del d.lgs. 196/2003 e quindi deve trattarsi di soggetti individuati tra quelli che, per esperienza, capacità, affidabilità nonché competenze tecniche, forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di dati personali. Rileva, inoltre, l'effettivo passaggio di mansioni dal titolare al responsabile. Il responsabile non deve essere un mero esecutore del titolare ma al contrario deve avere autonomia gestionale, poteri e mezzi sufficienti per imporne l'adempimento

all'interno dell'azienda. Il responsabile deve in modo consapevole accettare le responsabilità e gli obblighi derivanti dalla delega. Per questo motivo è necessaria una specifica fase di informazione/formazione del responsabile prima del conferimento e dell'accettazione dell'incarico (ERCOLANO).

Alla base della piramide dell'organigramma privacy vi è la figura necessaria degli incaricati. Infatti, come puntualizzato in precedenza le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

A differenza di quanto esaminato nel caso di nomina del responsabile, nell'ipotesi di nomina degli incaricati ci troviamo di fronte ad una condizione formale necessaria per il trattamento dei dati personali (ERCOLANO) e non di una vera e propria delega di funzioni (DI RAGO). La designazione deve essere fatta per iscritto e spetta al titolare o al responsabile individuare in modo specifico l'ambito di trattamento. L'incaricato ha il dovere di effettuare il trattamento basandosi su tali prescrizioni e rimane soggetto al potere di vigilanza e controllo esercitato dal titolare e/o responsabile. La nomina non comporta altro che una formalizzazione necessaria che nulla aggiunge in tema di mansioni e/o incarichi lavorativi. La conseguenza di un eventuale rifiuto della nomina determinerebbe

l'impossibilità di trattare i dati personali e nei casi in cui questo trattamento sia essenziale allo svolgimento del lavoro diventa impossibile poter esplicitare le proprie mansioni. Merita attenzione il punto 19.6 dell'allegato B al Codice in materia di predisposizione delle misure minime di sicurezza nell'ambito del trattamento dei dati personali sensibili e giudiziari che impone al titolare e/o responsabile la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione deve essere programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

La lettera d'incarico e la formazione sono momenti imprescindibili per una sensibilizzazione e responsabilizzazione degli incaricati. Solo una partecipazione effettiva e consapevole dell'incaricato alle politiche di sicurezza dell'ente può accrescere la sicurezza complessiva del trattamento ed essere fonte di una eventuale responsabilità dello stesso.

Oltre ai soggetti espressamente previsti dal Codice, il titolare del trattamento può intravedere la necessità di nominare e/o identificare altre figure per poter svolgere in sicurezza il trattamento dei dati. Si pensi, ad esempio, al c.d. **amministratore di sistema** chiamato a gestire le esigenze informatiche legate al trattamento dei dati con strumenti elettronici (installazione e aggiornamento dei sistemi operativi, degli applicativi necessari allo svolgimento delle attività lavorative, dei programmi antivirus, firewall e degli altri software necessari a limitare i rischi di intrusioni informatiche). A quest'ultima figura si aggiunge il **custode delle copie delle credenziali di autenticazione e l'incaricato della custodia delle copie di sicurezza delle banche dati**. Compito del primo è quello di provvedere alla conservazione in luogo sicuro, senza divulgarle, tutte le parole chiave o qualsiasi altra credenziale di autenticazione ai sistemi informatici fornita ad ogni incaricato al trattamento; compito del secondo, invece, è quello di adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al back-up periodico degli stessi con copie di sicurezza, secondo i criteri stabiliti dal titolare e/o dal responsabile ai sensi del Codice e del relativo disciplinare tecnico (ERCOLANO; BERGHELLA).

A capo di questi soggetti può essere nominato dal titolare uno specifico responsabile della sicurezza che stabilisca le corrette policy

e procedure di gestione cui essi devono attenersi; queste funzioni possono, invero, essere svolte direttamente dal titolare o dal responsabile di trattamento, nel caso in cui posseggano adeguate competenze tecniche. Per concludere sul punto si può rapidamente affermare che la responsabilità nell'ambito di un ente pubblico o privato è strettamente connessa al ruolo che il soggetto riveste in seno all'organico privacy e in particolare ai compiti che a ciascuno sono stati affidati e consapevolmente accettati.

Infine, è necessario brevemente segnalare che lo stesso Garante per la protezione dei dati personali procede all'identificazione di figure ulteriori rispetto a quelle individuate espressamente dal Codice in base alle esigenze che la prassi evidenzia. Nell'ambito della rilevazione di impronte digitali ed immagini presso gli istituti di credito, ad esempio, assume un ruolo di estrema rilevanza la figura del vigilatore. Tale figura è così identificata: «il vigilatore dei dati (individuato nel titolare di una funzione di controllo interno in posizione di indipendenza, o da un soggetto parimenti indipendente da questi designato), è il depositario delle chiavi crittografiche idonee a decifrare le informazioni conservate dalla banca» (Provvedimento “Istituti di credito - Rilevazione di impronte digitali ed immagini: limiti e garanzie” del 27 ottobre 2005, G.U. n. 68 del 22.3.2006). In estrema sintesi vigilatore dei dati è «...un soggetto

indipendente dalla banca a cui viene affidato un compito importante a difesa dei cittadini. A questa nuova figura spetta il delicato ruolo di custodire le chiavi crittografiche e di garantire la riservatezza dei clienti» (FORTUNATO).

Sintetizzando quanto affermato in tema di organigramma privacy nell'ambito della Pubblica Amministrazione ed utilizzando come fonte interpretativa quanto contenuto nella Direttiva 11.2.05, n. 1 della Presidenza del Consiglio dei ministri – Dipartimento della Funzione Pubblica – si evince quanto segue:

- per quanto riguarda i soggetti che effettuano il trattamento, l'art. 28 chiarisce che il titolare del trattamento, nel caso delle pubbliche amministrazioni, coincide con l'entità nel suo complesso ovvero con l'unità o l'organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza, anziché con la persona fisica incardinata nell'organo o preposta all'ufficio;
- per quanto riguarda la designazione di uno o più responsabili del trattamento ex art. 29 del Codice, questi devono essere individuati fra i soggetti che, per qualità

professionali e personali, forniscano idonea garanzia del rispetto delle disposizioni vigenti in materia; la designazione in esame deve essere corredata dalla specificazione analitica per iscritto dei compiti affidati e dalla vigilanza periodica sulla puntuale osservanza delle istruzioni impartite e sul generale rispetto delle norme in materia di protezione dei dati personali, come previsto dal comma 5 dell'art. 29;

- per quanto riguarda gli incaricati del trattamento questi ultimi operano sotto la diretta autorità del titolare o del responsabile, previa designazione espressa per iscritto, contenente la puntuale individuazione dell'ambito del trattamento loro consentito e l'indicazione delle istruzioni cui devono attenersi nello svolgimento del trattamento.

9. L'INTERESSATO E I SUOI DIRITTI

L'interessato è la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali (art. 4, comma 1 lett. i, del Codice).

Ai fini del trattamento dei dati personali, come disciplinato dalla legge 31 dicembre 1996, n. 675 (e quindi dal d.lgs. 30 giugno 2003, n. 196), e dell'esperimento della tutela predisposta dagli artt. 1 e seguenti, perchè una persona assuma la qualità di "interessato" è necessario che i dati di cui si controversa riguardino la persona fisica o la persona giuridica o l'ente o l'associazione che si dolga proprio del loro trattamento, non essendo richiesto che i dati appartengano, con certezza, alla persona che si duole delle operazioni compiute su di essi, atteso che quel che rileva è la loro attribuzione o la loro esclusione rispetto a colui che, al riguardo, accampi un diritto (alla titolarità ovvero all'estraneità' dei dati). Pertanto, anche l'inesatto trattamento dei dati consente di invocare, presso la competente autorità di garanzia la tutela apprestata dalla legge, il cui disegno è funzionale alla difesa della persona e dei suoi fondamentali diritti e tende ad impedire che l'uso, astrattamente legittimo, del dato personale avvenga con modalità tali da renderlo lesivo di quei diritti: qualora, perciò, si contesti l'attribuzione alla propria persona di determinate immagini, non ci si spoglia, per ciò stesso, della qualità di "interessato", perchè proprio il fatto che il soggetto intenda escludere l'attribuzione a sè di quei dati iconici comporta che egli abbia assunto, a ragione, quella qualificazione e,

in forza di essa, possa chiedere (nella specie, al Garante e quindi al Tribunale) l'adozione di provvedimenti (qui, blocco del trattamento e distruzione dei dati).

(Cass. civ., sez. I, 8.7.05, n. 14390 in CED RV584964)

Dopo aver sancito il principio per cui «chiunque ha diritto alla protezione dei dati personali che lo riguardano», il legislatore dedica il Titolo II della prima parte del Codice all'approfondimento dei diritti del soggetto a cui si riferiscono i dati oggetto del trattamento, l'interessato. Si tratta di una serie di diritti che consentono l'esercizio di un potere effettivo di controllo sull'utilizzo dei dati.

Il primo e concreto diritto dell'interessato è quello di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile (art. 7, primo comma, del Codice). L'interessato ha così diritto di ottenere anche in via preventiva la conferma dell'esistenza di un trattamento di dati che si riferiscono alla sua persona. Al fine di garantire un'effettiva capacità di controllo, il legislatore sottolinea il fatto che la comunicazione, in risposta al quesito dell'interessato, debba essere fornita in modo comprensibile al fine di far individuare facilmente il tenore della risposta. Il titolare del trattamento, quindi, è tenuto a dare un riscontro alla suddetta richiesta anche nell'ipotesi di esito negativo. L'interessato ha diritto di ottenere tutta una serie di

informazioni relative al reperimento, registrazione, archiviazione e utilizzo dei suoi dati. Si tratta di un controllo sulla qualità e quantità dei dati trattati che si configura come momento necessario e propedeutico per poter esercitare gli ulteriori diritti tesi ad eliminare o quantomeno limitare gli eventuali danni provocati da un trattamento illecito (art. 7, secondo comma, del Codice). In particolare, l'interessato ha diritto di conoscere: a) l'origine dei dati personali; b) le finalità e modalità del trattamento; c) la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) gli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2, del Codice; e) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

La comunicazione all'interessato in merito alle predette richieste, a pena di violazione del diritto di accesso ai dati personali, non possono essere rese in forma generica e senza uno specifico e puntuale riscontro. Le richieste indicate non devono essere giustificate e/o motivate in quanto il diritto riconosciuto dal Codice all'interessato non è in alcun modo subordinato all'indicazione di particolari motivazioni. Da quanto affermato si può notare una delle

più rilevanti differenze, che verranno approfondite nel prosieguo della trattazione, tra diritto di accesso ai dati personali ex d.lgs. 196/03 e diritto di accesso alla documentazione amministrativa ex legge 241/90. L'interessato non ha solo il diritto di conoscere se, quali e come i suoi dati vengono trattati ma ha anche il diritto di ottenere (art. 7, comma 3, del Codice) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei stessi. Esercitando tali diritti l'interessato può rendere attuali i propri dati correggendo eventuali errori e/o integrando gli stessi con ulteriori e nuove informazioni. L'interessato può esercitare il dominio pieno sui propri dati anche attraverso la richiesta di cancellazione, trasformazione in forma anonima o il blocco - ossia la conservazione di dati personali con sospensione temporanea di ogni altra operazione - dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati. L'interessato ai sensi dell'art. 7, ultimo comma, del Codice ha diritto di opporsi, in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di

comunicazione commerciale. Nella prima ipotesi indicata, ossia quando ricorrono motivi legittimi, l'interessato ha diritto di opporsi al trattamento anche nel caso in cui il trattamento non è in sé illecito. Il legislatore impone quindi di compiere un bilanciamento tra gli opposti interessi del titolare e dell'interessato consentendo però a quest'ultimo di prevalere nel caso in cui i motivi siano fondati su giusti e legittimi diritti.

Il legislatore indica in modo minuzioso anche le modalità attraverso cui i predetti diritti possono essere esercitati. L'art. 8 del Codice dispone che i diritti di cui all'art. 7 del Codice devono essere esercitati con una richiesta al titolare o al responsabile. Da un punto di vista formale tale richiesta non deve possedere particolari requisiti o forme. Il riscontro all'istanza inoltrata dall'interessato deve essere fornito senza ritardo non potendo essere la stessa lasciata inevasa.

Tuttavia, l'esercizio dei diritti di cui all'articolo 7 non può realizzarsi con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145 del Codice, se i trattamenti di dati personali sono effettuati: a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio; b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18

febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive (normativa antiracket); c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione, tali Commissioni procedono alle indagini e agli esami con gli stessi poteri e le stesse limitazioni dell'autorità giudiziaria; d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità; e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria, tuttavia tali esigenze devono essere dimostrate; f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397; g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della

giustizia; h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1° aprile 1981, n. 121.

Nei casi elencati non è più sufficiente inoltrare la richiesta al titolare ma è necessaria una segnalazione al Garante che provvederà, nell'ambito dei poteri di accertamento e controllo secondo quanto disposto dagli articoli 157 e seguenti del Codice alla verifica dell'esistenza dei suddetti presupposti. In questa palese limitazione all'esercizio dei diritti dell'interessato si cela un bilanciamento di interessi tra i predetti diritti ed alcune esigenze di natura pubblicistica che il legislatore ha identificato come superiori (DI MARTINO – VOLTAN).

Interessanti al fine di esplicitare il contenuto della predetta normativa si rivelano le conclusioni raggiunte dal Tribunale di Patti secondo il quale alla Banca d'Italia non si può ordinare in via d'urgenza la cancellazione di un'iscrizione a sofferenza nella Centrale dei rischi. Il motivo di tale principio risiede nel disposto dell'art. 8 del d.lgs. 30 giugno 2003, n. 196, secondo cui i diritti di cancellazione dei dati non possono essere esercitati nei confronti dei soggetti pubblici che raccolgono dati per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari,

nonché alla tutela della loro stabilità (Tribunale Patti, ord. 16.5.2005 in *il Corriere del Merito*, 2005, 8/9, 881)

L'ultimo comma dell'art. 8 conclude affermando che l'esercizio dei diritti suesposti quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

Per quanto riguarda le modalità di esercizio dei diritti (art. 9 del Codice) il legislatore tende a realizzare una disciplina tesa alla semplicità ed alla speditezza. La richiesta può essere trasmessa, infatti, anche mediante lettera raccomandata, telefax o posta elettronica e quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile. Nell'esercizio dei suoi diritti l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi ed inoltre l'interessato può, altresì, farsi assistere da una persona di fiducia. E' necessario puntualizzare che sempre ai sensi dell'art. 9 del Codice, la persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta

in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti. Per quanto riguarda i diritti di cui all'articolo 7 del Codice riferiti a dati personali concernenti persone decedute tali diritti possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento.

Al fine di garantire un effettivo esercizio dei diritti dell'interessato il titolare del trattamento deve adottare, ai sensi dell'art. 10 del Codice, delle misure idonee volte ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili. Il titolare deve inoltre procedere alla semplificazione delle modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico. I dati richiesti devono essere estratti a cura

del responsabile o degli incaricati e il risultato di tale ricerca può essere comunicata al richiedente anche oralmente ovvero offerta in visione mediante strumenti elettronici. La semplice comunicazione orale o l'offerta in visione sono comunque subordinati alla reale e concreta agevole comprensione dei dati. Tale facilità di comprensione deve essere considerata principalmente anche in rapporto alla qualità e alla quantità delle informazioni.

Nel caso in cui l'avente diritto richiede copia dei suddetti dati sarà cura del responsabile provvedere alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica. E' necessario puntualizzare che quando la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1, « I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a), da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare.»

Il legislatore si sofferma su un altro carattere della comunicazione: la comprensibilità. Infatti, l'interessato ha diritto ad una comunicazione in forma intelligibile dei dati «anche attraverso l'utilizzo di una grafia comprensibile». Nel caso in cui la

comunicazione o parte di essa sia costituita da codici o sigle la loro spiegazione deve essere fornita, anche mediante gli incaricati.

In merito alla titolarità del diritto alla protezione dei dati personali si riportano le conclusioni a cui è giunto il Consiglio di Stato in una sentenza del febbraio 2006:

...la privacy è un diritto inviolabile riconosciuto a chiunque, ma, proprio perché si tratta di privacy, limitatamente a fatti, dati e notizie che riguardano in via immediata e diretta il soggetto. Il Codice della protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196) dispone che chiunque ha diritto alla protezione dei dati personali che lo riguardano (art. 1), e tale diritto può essere esercitato o in prima persona, o tramite terzi soggetti (ivi compresi enti o associazioni), purché muniti di specifica delega o procura scritta (art. 7). Il Codice citato detta inoltre specifiche disposizioni relative al trattamento dei dati personali giudiziari (artt. 20, 21, 22). Coerentemente, lo statuto dei consumatori non riconosce ai consumatori in quanto tali, né a loro associazioni, il diritto alla privacy (art. 2 Codice del consumo approvato con d.lgs. n. 206/2005), proprio perché si tratta di diritto individuale del soggetto (persona fisica o anche ente giuridico), insuscettibile di una azione di categoria, e dunque di una azione da parte del Codacons, in difetto di specifica delega o procura scritta da parte degli interessati.

(Cons. Stato, sez. VI, 10.2.06, n. 555)

10. IL TRATTAMENTO DEI DATI PERSONALI: LE REGOLE GENERALI E LE RESPONSABILITÀ DA TRATTAMENTO ILLECITO

Il legislatore del Codice puntualizza nell'art. 4 del Codice che per **"trattamento"** si deve intendere una 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 (dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione), la diffusione (dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione), **la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.** Si desume in via preliminare che il "trattamento" dei dati avviene anche attraverso l'utilizzo di strumenti diversi da quelli elettronici ed informatici. Il trattamento dei dati inizia nel momento stesso in cui i dati vengono raccolti e continua ad essere

posto in essere in tutte le fasi successive dalla registrazione ed organizzazione sino alla loro cancellazione e distruzione. Al fine di definire la disciplina nell'ambito delle strutture pubbliche è necessario preliminarmente ripercorrere le regole generali sul trattamento dei dati per poi soffermarsi sulle regole ulteriori che il Codice detta per i soggetti pubblici. Mutuando i principi contenuti nell'art. 5 della Convenzione di Strasburgo n. 108/1981 e nell'art. 6 della direttiva 95/46/CE, l'art. 11 del Codice, dispone che i dati personali oggetto di trattamento devono essere trattati in modo lecito e secondo correttezza. In tale prospettiva, i dati devono essere raccolti e registrati per scopi determinati, espliciti e legittimi, e possono essere utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi. Un'ulteriore qualità è quella dell'esattezza in quanto anche questa caratteristica deve essere assicurata con particolare attenzione e se risulta necessario attraverso un'operazione di aggiornamento. Infine, i dati trattati devono risultare pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati. Per quanto riguarda la conservazione, i dati trattati devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. Il fine informa di sé,

quindi, l'intero periodo di trattamento rappresentando l'obiettivo e il fondamento di ogni operazione sui dati personali. La stessa liceità del trattamento dipende dallo scopo per il quale i dati sono trattati.

In ossequio al principio di "non eccedenza", il Tribunale di Messina ha ritenuto che ai fini della convocazione del Consiglio Comunale sia stata ritenuta eccedente la menzione del nome della persona interessata poiché non necessaria ai fini della validità della convocazione stessa. In altre parole il Tribunale di Messina mette in evidenza il principio per cui un trattamento dei dati è eccedente in rapporto alle sue finalità nel momento in cui lo stesso trattamento non sia necessario per la validità dell'atto per il quale è stato realizzato (Tribunale Messina, 7.11.05, in *il Corriere del Merito*, 2006, 2, 159).

I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Il rispetto di questi principi è rilasciato a forme di autoregolamentazione in ossequio ai dettami comunitari (cfr. art. 27 Direttiva 95/46/CE) diretti ad incoraggiare l'elaborazione di codici di condotta destinati a contribuire, in funzione della specialità settoriali alla corretta applicazione delle disposizioni nazionali di attuazione della già citata direttiva (DI MARTINO – VOLTAN). Si tratta di

una scelta diretta a produrre negozialmente il diritto coinvolgendo in modo preventivo e diretto le categorie coinvolte. In tale prospettiva l'art. 12 del Codice così dispone: «Il Garante promuove nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verifica la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto. I codici sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, sono riportati nell'allegato A) del presente Codice. Il rispetto delle disposizioni contenute nei codici di cui al comma 1 costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici. Le disposizioni del presente articolo si applicano anche al Codice di deontologia per i trattamenti di dati per finalità giornalistiche promosso dal Garante nei modi di cui al comma 1 e all'articolo 139».

Con specifico riferimento all'attività giornalistica, la legge n. 675, come risulta da un complesso di disposizioni ad essa appositamente dedicate, stabilisce il principio cardine della libertà del trattamento.

Secondo l'art. 25, comma 1, "le disposizioni relative al consenso dell'interessato e all'autorizzazione del garante, nonché il limite previsto dall'art. 24, non si applicano quando il trattamento dei dati di cui agli articoli 22 e 24 è effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità". E la disposizione prosegue, più in generale, affermando che "Il giornalista rispetta i limiti del diritto di cronaca, in particolare quello dell'essenzialità dell'informazione ... ferma restando la possibilità di trattare i dati relativi a fatti resi noti direttamente dall'interessato o attraverso i suoi comportamenti in pubblico". Inoltre, si stabilisce (commi 2 e 4) che un apposito Codice deontologico, promosso dal garante ed adottato dal Consiglio nazionale dell'ordine dei giornalisti e pubblicato sulla Gazzetta Ufficiale, conterrà "misure ed accorgimenti a garanzia degli interessati rapportate alla natura dei dati, in particolare per quelli idonei a rivelare lo stato di salute e la vita sessuale", ma anche prescrizioni concernenti i dati personali meno invasivi e, comunque, diversi da questi. Com'è noto, il Codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica è stato adottato con Provvedimento del garante del 29 luglio 1998 ed è stato pubblicato nella G.U. del 3 agosto 1998, n. 179. In esso sono regolate anche le banche dati di uso redazionale e gli archivi personali dei giornalisti (art. 2), nonché, più in generale, i principi che sovrintendono al trattamento delle informazioni che devono alimentare l'attività professionale, la cui specificità è rivendicata con decisione (perché, "la raccolta, la registrazione, la conservazione e la diffusione di notizie ..., attuate nell'ambito dell'attività giornalistica e per gli scopi propri di tale attività, si differenziano

nettamente per la loro natura dalla memorizzazione e dal trattamento di dati personali ad opera di banche dati o altri soggetti": art. 1, co. 2), in ossequio al "diritto all'informazione su fatti di interesse pubblico", ma anche nel contemperamento con il canone "dell'essenzialità dell'informazione" (art. 5, co. 1, ult. parte e art. 6) e la tutela di alcuni particolari soggetti (il minore, art. 7; il malato, art. 10) e comunque, sempre, della dignità delle persone (art. 8) e della sua sfera sessuale (art. 11). Il rispetto di tali previsioni deontologiche, che è espressamente riferito anche ai giornalisti (art. 12 D. Lgs n. 196 del 2003 e, prima ancora, art. 20 D. Lgs. n. 467 del 2001) ed è "condizione essenziale per la liceità e la correttezza del trattamento dei dati personali" (art. 12, comma 3, D. Lgs. n. 196 cit.), non solo può dar luogo a provvedimenti disciplinari, (che è cosa che in questa sede non rileva) ma, soprattutto, consente al garante di adottare tutta la gamma dei provvedimenti delineati dalla legge sulla privacy.

(Cass. civ., sez. I, 25.6.04, n. 11864)

Il momento iniziale del trattamento dei dati personali si fonda sull'informativa, un atto orale o scritto, attraverso cui l'interessato è informato in merito alle finalità della raccolta dei dati ed alle modalità di trattamento degli stessi una volta acquisiti. In tal modo l'interessato ha una chiara ed immediata percezione della raccolta e degli scopi per i quali le informazioni relative alla sua persona vengono raccolti e trattati e potrà così esercitare un effettivo controllo preventivo sulle operazioni trattamento realizzate sui dati

personali. L'informativa deve anche esplicitare la natura obbligatoria o facoltativa del conferimento dei dati, ossia il titolare del trattamento ha l'obbligo di indicare quali dati sono strettamente necessari per l'esercizio dell'attività e quali al contrario non sono ad essa necessari. L'interessato potrà così esercitare il suo diritto di scelta in merito alla concessione dei dati personali che non risultano strettamente necessari. A tal fine, si devono indicare le conseguenze di un eventuale rifiuto di rispondere a determinate richieste di dati in modo da mettere ancora in maggior evidenza il discrimine tra dati necessari e facoltativi. Tra le altre informazioni che deve contenere l'informativa vi sono anche quelle relative ai soggetti o alle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi. Il legislatore del Codice ha voluto con tale disposizione obbligare il titolare a rendere noti i suoi estremi identificati e, se designati, quelli del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Infine, l'informativa deve contenere l'indicazione dei diritti esercitabili dall'interessato ai sensi dell'articolo 7 del Codice. E' necessario puntualizzare che sono tenuti al rilascio dell'informativa tanto i soggetti privati quanto i soggetti pubblici. L'informativa deve contenere oltre alle informazioni in precedenza indicate anche gli

elementi previsti da specifiche disposizioni del Codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

Per non creare inefficienze nell'ambito dei servizi telefonici di assistenza ed informazione al pubblico, il Garante può individuare delle modalità semplificate per fornire l'informativa agli interessati. Nel caso in cui i dati non siano raccolti presso l'interessato deve essere fornita al momento della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione. La predetta disposizione non si applica quando i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria oppure quando i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento oppure, infine, quando il fornire l'informativa all'interessato comporti un impiego di mezzi che il Garante reputi manifestamente sproporzionati rispetto al diritto

tutelato ovvero impossibile. Particolare attenzione merita il trattamento di quei dati, diversi da quelli sensibili e giudiziari, che presentano ontologicamente una serie di rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare. In tali casi il trattamento è ammesso solo se realizzato nel rispetto di una serie di misure ed accorgimenti posti in essere a garanzia dell'interessato nel caso in cui il Garante li prescriva in applicazione dei principi sanciti dal presente Codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare (art. 17 del Codice). Sul punto, come un'accorta dottrina mette in evidenza, si può notare che le disposizioni citate nel caso di trattamento soggetti a rischi specifici riproponga il contenuto dell'art. 24 bis della legge 675/1996 riferendosi alla categoria dei c.d. dati semi-sensibili (LISI – BERTONI). Infine, il Codice all'art. 16 detta le regole generali che devono disciplinare la cessazione del trattamento dei dati, prescindendo dalla causa che l'ha determinata. In tale ipotesi i dati devono, alternativamente, essere distrutti, ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti; conservati per fini esclusivamente

personali e non destinati ad una comunicazione sistematica o alla diffusione; conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 12 del Codice. Una particolare attenzione nell'ambito delle attività svolte dalla Pubblica Amministrazione deve essere attribuita a quanto disposto dall'art. 14 del Codice in merito alla **definizione di profili e della personalità dell'interessato**: «Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato. L'interessato può opporsi ad ogni altro tipo di determinazione adottata sulla base del trattamento di cui al comma 1, ai sensi dell'articolo 7, comma 4, lettera a), salvo che la determinazione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dal presente Codice o da un provvedimento del Garante ai sensi dell'articolo 17».

La forza di tale assunto è molte volte sottovalutata da una lettura rapida dell'impianto normativo del Codice. Essendo la Pubblica

Amministrazione un archivio di archivi è ad essa espressamente vietato fondare l'adozione atti, provvedimenti giudiziari o amministrativi che sottintendano una valutazione del comportamento umano su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato. Il valore di tale principio non è quello di limitare e rendere sicure le c.d. operazioni di profilazione dell'utente per fini, in ampio senso, commerciali ma è quello più generale di affermare il diritto di non essere sottoposto ad una decisione che produca effetti rilevanti basata esclusivamente su una valutazione fondata su un profilo della persona dell'interessato realizzato in modo automatico attraverso l'elaborazione e lo studio dei suoi dati personali.

Il legislatore impone a chiunque cagioni un danno per effetto del trattamento di dati personali di risarcire lo stesso ai sensi dell'articolo 2050 del Codice civile. Tale norma individua il fondamento della responsabilità derivante dall'esercizio di attività pericolose: **«Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee ad evitare il danno».**

Per l'individuazione dei caratteri essenziali della categoria "attività pericolose", in cui il legislatore fa rientrare il trattamento dei

dati personali, è di estrema utilità ripercorrere alcune recenti massime della Corte di Cassazione:

L'art. 2050 cod. civ., partendo dal presupposto logico che tutte le attività umane contengono in sé un grado più o meno elevato di pericolosità per coloro che le esercitano, prende in considerazione solo quelle di per sé potenzialmente dannose per l'alta percentuale di danni che possono provocare, in ragione della loro natura o per la natura dei mezzi adoperati, assoggettandole al giudizio di responsabilità indicato dalla norma: in questo senso, Cass. 15 ottobre 2004, tra le più recenti. Nell'ambito della norma si possono inquadrare anche gli eventi dannosi collegati ad un comportamento omissivo, a condizione che si tratti di omissione qualificata, come accade quando il soggetto non adotti misure preventive del verificarsi dei danni alle quali sia tenuto per legge o per contratto. Naturalmente, presupposto del riconoscimento del danno è l'esistenza di un nesso di causalità tra l'attività pericolosa e l'evento di danno, riconducibili all'esercente, come questa Corte ha costantemente ritenuto (Cass. 4.5.04, n. 847, tra le più recenti). In altri termini, si deve trattare di una relazione diretta tra danno e rischio specifico dell'attività pericolosa o dei mezzi adoperati, giacché, diversamente, il danno cagionato può essere riconosciuto solo in base al criterio generale dell'art. 2043 cod. civ., se ne ricorrono i presupposti di applicazione.

(Cass. civ., sez. III, 21.10.05, n. 20359)

Per attività pericolose, in relazione al cui svolgimento l'art. 2050 Cod. Civ. stabilisce una presunzione di responsabilità a carico di chi le esercita, devono intendersi quelle che tali sono qualificate dalla legge di P.S. e da altre norme speciali come quelle sugli infortuni sul lavoro ed altresì quelle che abbiano insite la pericolosità nei mezzi adoperati e nella loro stessa natura, talché non può considerarsi pericolosa agli effetti dell'art. 2050 Cod. Civ. l'attività bancaria, perché i rischi cui sono esposti i clienti negli istituti di credito in relazione alle azioni di malviventi non derivano dalla natura dell'attività bancaria, potendo la stessa costituire soltanto l'occasione per tali rischi.").

(Cass. civ., sez. III, 27.5.05, n. 11275)

Il superamento della presunzione di responsabilità a carico del danneggiante ex art. 2050 c.c. presuppone l'accertamento preventivo dell'esistenza del nesso causale tra l'esercizio di tale attività e l'evento dannoso. La prova di questo legame eziologico spetta al danneggiato e non al presunto danneggiante (Cass. 17.7.02 n. 10382). Tuttavia, incombe sull'esercente dell'attività pericolosa l'onere di provare di aver adottato tutte le misure idonee a prevenire il danno (Cass. 4.12.98, n. 12307 in Foro it., 1999, I, 1938). Tale presunzione di responsabilità può essere vinta, però, attraverso una prova particolarmente rigorosa capace di dimostrare che il danneggiante abbia adottato le suddette misure idonee non essendo in alcun modo sufficiente la prova negativa di non aver commesso

violazione alcuna di norme di legge e/o di prudenza. E' necessaria, in altre parole, una prova positiva di aver prestato nell'esercizio di tale attività pericolosa ogni cura necessaria per impedire l'evento dannoso. In questa prospettiva anche il fatto del danneggiato o del terzo produce degli effetti liberatori solo ed esclusivamente se tali effetti sono idonei ad escludere il nesso causale tra attività ed evento dannoso. Nell'ipotesi in cui i suddetti fatti costituiscano invece delle semplici concause concorrenti nella produzione del danno tale responsabilità non è esclusa (Cass. 4.6.98 , 5484).

...la responsabilità ex art. 2050 c.c. rientra nelle figure di responsabilità oggettiva, vale a dire quelle forme di responsabilità che prescindono dalla colpa del responsabile. La responsabilità viene fatta gravare su chi ha posto in essere l'attività, senza riguardo all'eventuale colposità del proprio comportamento, come nell'ipotesi di cui all'art. 2051 c.c. Pur differenziandosi le norme in esame per il fatto che in un caso il danno deriva dall'attività e nell'altro dalla cosa, nulla esclude che il danno sia imputabile al soggetto quale esercente un'attività pericolosa e quale custode di una cosa. Pertanto, al di là delle opinioni profilatesi in dottrina e in giurisprudenza, sarà compito dell'interprete valutare caso per caso l'operatività della presunzione di responsabilità prevista dall'art. 2050 c.c. piuttosto che quella di cui all'art. 2051 c.c., ricorrendo in particolare modo al carattere dinamico dell'attività o statico della res custodita. L'esercente l'attività pericolosa è assoggettato alla presunzione di responsabilità ai sensi dell'art. 2050 c.c. in relazione ai danni cagionati

nello svolgimento dell'attività, presunzione che lo stesso può vincere fornendo la dimostrazione di avere adottato tutte le misure idonee ad evitare il danno. Nella scelta di tali misure, egli dispone di un certo margine di discrezionalità, da esercitare facendo uso della normale prudenza e tenendo conto dello sviluppo della tecnica e delle condizioni pratiche in cui si svolge l'attività. Siffatta discrezionalità, peraltro, viene meno quando è la legge ad imporre l'obbligo di adottare talune misure. Pertanto, la presunzione di responsabilità opera nei confronti dell'esercente l'attività pericolosa che abbia adottato misure diverse da quelle prescritte da norme legislative (o regolamentari), senza che vi sia alcuna possibilità, in tal caso, di valutarne l'idoneità (Cass. 02/03/2001, n. 3022). Senonché, pur versandosi in ipotesi di presunzione di responsabilità e non di presunzione di colpa, essa pur sempre presuppone il previo accertamento dell'esistenza del nesso eziologico - la prova del quale incombe al danneggiato - tra l'esercizio dell'attività e l'evento dannoso, non potendo il soggetto agente essere investito da una presunzione di responsabilità rispetto ad un evento che, non è ad esso riconducibile.

(Cass. civ., sez. III, 4.5.04, n. 8457)

L'art. 15 secondo comma, del Codice dispone, inoltre, la risarcibilità del danno non patrimoniale anche nel caso di violazione dell'articolo 11 relativo alle modalità del trattamento e ai requisiti dei dati.

Sinteticamente si può affermare, che il danno non patrimoniale «consiste nella perdita o lesione di un bene personale, che non possa essere oggetto di scambio e di valutazione economica» (TRIMARCHI).

La risarcibilità del danno non patrimoniale - di regola conseguente all'illiceità penale della condotta da cui è derivato - non è esclusa in ulteriori ipotesi specificamente previste da disposizioni di legge, ad esempio in tema di tutela del consumatore o della privacy, o di diritto alla ragionevole durata del processo

(Tribunale Verbania, 23.4.02, in Giurisprudenza di merito, 2002, 6, I, 1193)

11. LE ULTERIORI REGOLE PER IL TRATTAMENTO DEI DATI DA PARTE DEI SOGGETTI PUBBLICI

Il Codice detta agli articoli 18 e seguenti una serie di regole aggiuntive per il trattamento dei dati da parte di tutti i soggetti pubblici, esclusi gli enti pubblici economici.

Nell'ambito della pubblica amministrazione è consentito il trattamento dei dati personali al fine di svolgere le funzioni istituzionali. In tale ambito, il trattamento di dati diversi da quelli sensibili e giudiziari è consentito anche in mancanza di una norma di legge o di regolamento che lo preveda in modo esplicito. Nel trattare i dati il soggetto pubblico deve osservare una cornice di presupposti e di limiti desumibili dal Codice, dalla legge e dai regolamenti. I soggetti pubblici non devono richiedere il consenso dell'interessato, salvo quanto previsto nella Parte II del Codice per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici.

Il TAR Lombardia ha ritenuto contrastante con la normativa contenuta negli artt. 11 e 18 del d.lgs. 196/2003, in quanto eccedenti le finalità del trattamento, la richiesta dell'Autorità per l'energia elettrica e il gas di informazioni relative ai fornitori esteri ed alle connotazioni dei contratti in corso, oltre che ai prezzi base di acquisto fob (free on board). I suddetti dati anche se non sono

riconducibili alla categoria di dati "sensibili" ex art. 4 del d.lgs. 196/2003 attengono prevalentemente alla sfera commerciale dell'impresa ricorrente e di conseguenza non possono reputarsi necessari all'esercizio, da parte dell'Autorità (T.A.R. sez. IV, Lombardia Milano, 1.12.2005, n. 4830).

Sempre in riferimento al **trattamento di dati diversi da quelli sensibili e giudiziari, ai sensi dell'art. 19 del Codice**, «la comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata». Tuttavia, è bene precisare che diversamente da quanto si è affermato per le comunicazioni di dati a privati o a enti pubblici economici e per la diffusione da parte di un soggetto pubblico queste sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Il Consiglio di Stato si è soffermato di recente sulla materia trattata giungendo ad affermare che:

L'art. 16, comma quinto, del D.P.R. 9.5.01, n. 244, recante la disciplina delle procedure istruttorie dell'A.E.E.G., stabilisce che l'atto finale del procedimento è comunicato "ai soggetti intervenuti nel procedimento" ed è "altresì pubblicato nel bollettino entro venti giorni dall'adozione". La norma di regolamento prevede, quindi, accanto ad una forma di comunicazione individuale a soggetti determinati dell'esito del procedimento (destinatario dell'atto finale e soggetti intervenienti) l'inserimento dello stesso in uno strumento (bollettino ufficiale) accessibile ad una cerchia indeterminata di soggetti, stante l'assenza di limiti quanto alla possibilità di replica e divulgazione del documento. Si realizza quindi, per espressa previsione della norma regolamentare attuativa dell'art. 2, comma 24, lett. a), della legge n. 481/1995, la "diffusione" dei dati contenuti nell'atto adottato dall'Autorità a soggetti diversi dal destinatario del provvedimento e che sono abilitati a conoscerli, senza discriminazioni, a mezzo del bollettino ufficiale dell'organismo di regolazione. Ciò che la Società appellata qualifica come "pubblicazione in internet" non integra in sé la "diffusione" dei dati personali contenuti nel provvedimento dell' A.E.E.G. - che è già avvenuta monte con la pubblicazione sul bollettino ufficiale - ma attiene allo strumento materiale (di carattere telematico e non solo cartaceo) attraverso il quale è possibile accedere alla conoscenza di un procedimento che, come in precedenza detto, è già assistito dalla condizione accessibilità ai "dati personali (da parte di) soggetti indeterminati", secondo la nozione di "diffusione" che si enuclea dall'art. 4, comma primo, lett. m), del d.lgs. n. 196/2003. L'A.E.E.G., pertanto, nel disporre l'inserimento nel proprio sito della delibera applicativa della misura sanzionatoria non è incorsa nella

violazione dell'art. 18, comma terzo, del d.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali).

(Cons. Stato, sez. VI, 16.3.06, n. 1412)

Per quanto riguarda il **trattamento dei dati sensibili e giudiziari** la disciplina si presenta più complessa ed articolata. I principi che devono ispirare il suddetto trattamento sono contenuti nell'art. 22 del Codice che si presenta come un vero e proprio vademecum per gli enti pubblici. Questi ultimi devono conformare il trattamento dei suddetti dati utilizzando delle modalità dirette a prevenire con appositi accorgimenti anche procedurali la violazione dei diritti, delle libertà fondamentali e della dignità dell'interessato. Per quanto riguarda l'informativa di cui all'art. 13 del Codice i soggetti pubblici devono fare espresso riferimento alla normativa che disciplina gli obblighi e i compiti posti a fondamento del suddetto trattamento. I dati sensibili e giudiziari trattati devono essere esclusivamente quelli indispensabili per svolgere le attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa. Spetta ai soggetti pubblici la verifica periodica dell'esattezza e dell'aggiornamento dei suddetti dati nonché la verifica della loro pertinenza, completezza, non eccedenza ed indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di

propria iniziativa. I soggetti pubblici hanno il dovere di trattare i dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, mediante tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. Anche in ambito pubblico, inoltre, i dati idonei a rivelare lo stato di salute e la vita sessuale devono essere conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. Quest'ultima tipologia di dati idonea a rivelare lo stato di salute non può essere diffusa. Il trattamento deve avvenire sempre avendo come obiettivo il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

Le disposizioni citate recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale.

Nell'ambito del trattamento dei dati sensibili da parte di soggetti pubblici rileva un recente caso giunto all'attenzione del Consiglio di Stato. La vicenda processuale prende le mosse dal ricorso proposto al TAR da un assistente della Polizia di Stato, che impugnava - chiedendone, previa sospensione, l'annullamento - il decreto con cui il Capo della Polizia aveva inflitto nei suoi riguardi la sanzione disciplinare della destituzione dal servizio, essendo risultato, in sede di accertamento medico-sanitario, positivo alla ricerca della cocaina e del suo principale metabolita: la benzoilecgonina.

... A sostegno del gravame, il ricorrente deduceva censure di violazione della legge n.675/1996 (artt.9, 10 e 17) e della legge n.196/2003 (artt.11, 13 e 14) nonché di eccesso di potere, sotto vari profili, rilevando, tra l'altro, che l'Amministrazione aveva ommesso di comunicargli i motivi della visita medica cui era stato sottoposto, procedendo al trattamento dei suoi dati personali in mancanza di qualsiasi contraddittorio. Per quel che rileva in questa sede il consiglio di Stato conclude sul punto così motivando: il d.lgs. 11.5.1999, n.135, concernente "Disposizioni integrative alla legge 31.12.1996, n.675, sul trattamento di dati sensibili da parte di soggetti pubblici", nello stabilire i principi generali e l'ambito di applicazione delle norme in materia di trattamento di dati particolari, individua, all'art.1, alcune rilevanti finalità di interesse pubblico, per il cui perseguimento è consentito detto trattamento, nonché le operazioni eseguibili e i tipi di dati che possono essere trattati, disponendo quindi

(all'art.16) che sono da considerarsi di rilevante interesse pubblico i trattamenti di dati volti all'applicazione di norme in materia di sanzioni amministrative e ricorsi (lett.a) e che siano necessari a far valere il diritto di difesa in sede amministrativa o giudiziaria (lett.c). Tra le finalità di rilevante interesse che consentono, appunto, il cennato trattamento, devono ricomprendersi dunque, come rettamente statuito dai primi giudici, pure le operazioni volte all'accertamento delle responsabilità, anche di natura disciplinare. Del resto, lo stesso D. Lgs. n.196 del 30.6.2003 (Codice in materia di protezione dei dati personali) ribadisce il possibile trattamento dei dati sensibili degli interessati in base ad un obbligo previsto dalla legge, da un regolamento o da una normativa comunitaria e, comunque, quando i dati sono trattati per far valere o difendere un diritto in sede giudiziaria. In conclusione, poiché il caso in esame riguardava il trattamento di dati volti all'applicazione di norme in materia di sanzioni, rientrante tra quelle aventi rilevante interesse pubblico, appaiono corrette le conclusioni a cui in proposito è pervenuto il Giudice di primo grado e, di converso, infondati i rilievi mossi al riguardo dalla parte appellante.

(Cons. Stato, sez. VI, 31.5.06, n. 3306)

In parte diverse sono, quindi, le regole applicabili al trattamento dei dati sensibili e giudiziari, ai sensi dell'art. 20 del Codice, il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se espressamente autorizzato da una disposizione di legge. In tale disposizione devono essere specificati i tipi di dati che possono essere trattati, le operazioni su di essi eseguibili e le finalità

di rilevante interesse pubblico perseguite che giustificano un tale trattamento.

Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo. Inoltre, se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì ad identificare e rendere pubblici i tipi di dati e di operazioni. Per quanto riguarda il trattamento di dati giudiziari da parte di soggetti pubblici, l'art. 21, primo comma, del Codice dispone che lo stesso è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che

specificchino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

Naturalmente, quanto affermato in merito alle regole aggiuntive in materia di trattamento dei dati personali deve essere letto alla luce del Codice dell'amministrazione digitale e dei diritti e delle modalità operative in esso esplicitati al fine di contemperare le esigenze di tutela dei dati personali con quelle dell'innovazione informatica della Pubblica amministrazione.

12. LA SICUREZZA DEI DATI PERSONALI NELL'AMBITO DELLA PUBBLICA AMMINISTRAZIONE TRA MISURE DI SICUREZZA E RESPONSABILITA'

L'entrata in vigore del D.Lgs. 196/03 riporta in evidenza il problema del trattamento dei dati da parte delle Pubbliche Amministrazioni. In questa sede appare opportuno soffermarsi sulle ragioni di fondo per cui è necessario pensare alla sicurezza dei dati personali non come una serie ulteriore di balzelli burocratici che si aggiungono magmaticamente a quelli preesistenti, ma come il necessario adattamento delle amministrazioni pubbliche alle nuove esigenze provenienti dalla moderna vita di relazione. La società dell'informazione è costituita, infatti, da una fitta rete di rapporti e di relazioni interpersonali, reali e virtuali, in cui l'elemento base è costituito dall'informazione. Alla luce della pacifica considerazione che le innovazioni tecnologiche hanno prodotto contemporaneamente risultati positivi di estremo rilievo ed, inevitabilmente, la nascita di nuove ed insidiose fonti di pericolo, meritano estrema tutela, a causa della loro rilevanza, le informazioni personali. Tuttavia, i maggiori rischi sono legati al reperimento ed all'uso illecito delle "tracce" (dati) personali che quotidianamente, consapevolmente e non, vengono spesi per ottenere servizi pubblici e

privati. Per quanto detto, occorre formare e diffondere una nuova coscienza ed una diversa concezione delle responsabilità legate alla gestione dei dati personali propri ed altrui. Da questa “politica di sicurezza”, a cui è strettamente connesso il bene “fiducia”, non possono essere esonerate le pubbliche amministrazioni che, per ragioni istituzionali, entrano continuamente in contatto con dati personali di estrema rilevanza e la cui illecita diffusione potrebbe cagionare un grave nocumento ai soggetti cui si riferiscono. In questa prospettiva in cui lo stesso svolgersi fisiologico della funzioni istituzionali presuppone il reperimento e l’archiviazione di dati personali, la Pubblica Amministrazione non può ritenersi esonerata dall’osservare le norme relative alla custodia ed al controllo dettate in materia. Il rapporto con i dati personali, a causa del loro intrinseco valore, deve essere scandito anche nell’esercizio dell’attività amministrativa dagli obblighi e dall’osservanza delle procedure imposte dal Codice. Ricapitolando brevemente quanto sino ad ora indicato, in primo luogo, occorre fornire le informazioni necessarie a giustificare la richiesta di determinati dati, quali ad esempio: a) le finalità e le modalità di trattamento, b) la natura obbligatoria o facoltativa del conferimento dei dati; c) le conseguenze di un eventuale rifiuto di rispondere; d) i soggetti o le categorie di soggetti che potranno venire a conoscenza dei dati comunicati; e) il diritto

dell'interessato di accedere ai propri dati, di aggiornarli o cancellarli. L'informativa diviene, così, un momento fondamentale del rapporto di fiducia che si instaura tra l'amministrazione e il cittadino e la successiva fase della raccolta dei dati forniti può ben essere intesa come il momento iniziale di quello che viene definito dallo stesso Codice con l'espressione: "trattamento di dati personali". Il secondo punto da osservare è di natura organizzativa e si riferisce all'individuazione nell'ambito della struttura del titolare, dei responsabili e dei soggetti incaricati del trattamento dei dati personali. La corretta individuazione di queste figure è un elemento essenziale per osservare correttamente i vari adempimenti e le procedure imposte dalla disciplina in questione. Si pensi, ad esempio, alla necessità di individuare le modalità organizzative idonee a soddisfare, in tempi brevi, le richieste provenienti dagli interessati di conoscere i dati personali archiviati ed eventualmente di modificarli o di cancellarli, oppure agli adempimenti in merito alla custodia degli archivi e del trattamento dei dati in esso contenuti da parte dei collaboratori. Ai sensi dell'art. 31 del Codice, inoltre, i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e

preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. A quanto superficialmente già considerato si deve aggiungere, in vista della capillare informatizzazione della Pubblica Amministrazione e del crescente bisogno di connessioni telematiche, l'adozione, necessaria e non più procrastinabile, di misure di sicurezza atte a tutelare i dati personali trattati e custoditi negli archivi informatici (si ricorda, comunque, che anche la raccolta cartacea, ad esempio in fascicoli, deve essere considerata un trattamento di dati personali). I dati personali devono essere difesi principalmente da tutte quelle vulnerabilità (non solo di natura tecnica ed informatica) che indeboliscono il sistema rendendolo potenzialmente soggetto ad attacchi e danneggiamenti.

Il Codice compie a tal proposito una distinzione delle misure di sicurezza in :

- **misure idonee** e preventive volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31)

- **misure minime**, indicate negli articoli 33-36 alla luce di quanto specificato nell'allegato B) (“Disciplinare tecnico in materia di misure minime di sicurezza”) al Codice.

La distinzione in esame ha notevoli ripercussioni nell’ambito delle responsabilità e del conseguente regime sanzionatorio.

Per quanto riguarda le misure minime, la disciplina è suddivisa in base al fatto che il trattamento venga effettuato con strumenti elettronici oppure senza l’ausilio degli stessi. Nella prima ipotesi è prevista l’adozione di un sistema di autenticazione informatica che consenta solo agli incaricati di poter procedere al trattamento dei dati custoditi nel sistema informatico, creando eventualmente diversi profili di autorizzazione per i casi in cui l’incaricato sia autorizzato a svolgere solo determinate operazioni. In considerazione delle normali e fisiologiche vulnerabilità presenti nei sistemi informatici, sono previsti degli obblighi relativi all’adozione di misure minime di sicurezza attraverso l’utilizzo di strumenti (software e hardware) e procedure tese:

- ad impedire l’accesso al sistema da parte di soggetti non autorizzati;

- ad impedire che i software dannosi (*virus, worm, trojan horse* ed altro *malware*) possano danneggiare i dati custoditi nel sistema;
- ad eliminare le vulnerabilità che periodicamente vengono rilevate nel software (sistema operativo ed applicativi) utilizzato;
- a compiere il *backup* dei dati (ossia la creazione di una copia di sicurezza di questi ultimi).

Agli accorgimenti di natura tecnica si deve aggiungere anche la redazione di un documento programmatico sulla sicurezza, obbligatorio per chi effettua un trattamento di dati sensibili e giudiziari con l'ausilio di strumenti elettronici, contenente idonee informazioni riguardo alla fenomenologia dei dati trattati, all'organizzazione e alle misure tecniche e procedurali adottate per garantirne la tutela e deve essere adottato, dall'organo, ufficio o persona fisica a ciò legittimata in base all'ordinamento dell'amministrazione Il D.P.S. deve contenere al suo interno l'analisi dei rischi che incombono sui dati personali, l'individuazione degli accorgimenti da adottare per prevenire la loro eventuale distruzione, perdita accidentale o gli accessi abusivi e la pianificazione degli interventi formativi nei riguardi del personale. Il termine per aggiornare annualmente il DPS è fissato alla scadenza del 31 marzo

di ogni anno, come dispone la regola tecnica n. 19 dell'allegato B) al Codice.

Inoltre, per quanto riguarda le modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici possono essere sintetizzate nel modo seguente. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione. Bisogna ricordare, infine, che ulteriori misure sono dettate in caso di trattamento di dati sensibili o giudiziari. Infatti, quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate. L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo,

dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

A conclusione di questa introduzione, necessariamente lacunosa, si può affermare che **la sicurezza dei dati personali all'interno della Pubblica Amministrazione** non può essere ridotta solo ed esclusivamente ad un fatto tecnico ma **deve essere intesa in senso più ampio come il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali**, tendenti a realizzare un livello di sicurezza proporzionato ai rischi previsti per l'attività in concreto esercitata.

13. LA PUBBLICA AMMINISTRAZIONE TRA DIRITTO DI ACCESSO E TRATTAMENTO DEI DATI PERSONALI

Il problema dell'applicabilità della normativa sulla tutela della riservatezza alle pubbliche amministrazioni si basa sulla soluzione di un potenziale conflitto tra il principio della trasparenza dell'azione amministrativa ed il principio della tutela della riservatezza.

Preliminarmente è necessario sottolineare alcune differenze che intercorrono tra il diritto di accesso ai documenti amministrativi e i diritti relativi alla protezione dei dati personali di cui il diritto di accesso ai dati è espressione.

Il diritto di accesso ai dati personali sancito dal Codice in materia di protezione dei dati personali è riferito appunto ai dati personali e non agli atti e documenti contenenti gli stessi. L'accesso a questi dati non richiede formalità specifiche e non subisce particolari limitazioni, salvo quelle indicate nello stesso Codice. Inoltre, è importante evidenziare che per esercitare il diritto di accesso ai dati personali, l'interessato non deve motivare le ragioni della richiesta di accesso. L'interesse ad accedere a tali informazioni è *in re ipsa*. Si tratta di un diritto pieno ed assoluto che riguarda però solo le informazioni relative alla propria persona e non può essere esteso a dati di terzi.

Il diritto di accesso ai documenti amministrativi, invece, è attualmente disciplinato in Italia dalla legge 7 agosto 1990 n. 241 (nel seguito, “Legge”), come recentemente modificata dalle leggi n. 15 e n. 80 del 2005. Tale diritto rappresenta per il cittadino uno strumento fondamentale di partecipazione al procedimento amministrativo, non soltanto in relazione ad un interesse “oppositivo”, mirante a contrastare una specifica attività amministrativa, ma anche in connessione ad un interesse di natura “pretensiva”, diretto cioè ad ottenere da parte dell’Amministrazione determinate prestazioni e/o servizi.

Il Consiglio di Stato con riguardo al diritto di accesso ai documenti amministrativi ha espressamente riconosciuto che:

...l'accesso ai documenti amministrativi così come regolato dagli art. 22 e 25 l. 7 agosto 1990 n. 241, si configura come un diritto soggettivo perfetto che può essere esercitato da chiunque vi abbia interesse, indipendentemente da ogni giudizio sull'ammissibilità o fondatezza della domanda giudiziale eventualmente proponibile sulla base dei documenti acquisiti mediante l'accesso.

(Consiglio di Stato, sez. VI, con sentenza 26.4.05, n. 1896)

Il diritto di accesso è, in questo senso, riconducibile a principi sanciti dalla nostra Carta costituzionale, quali: l'art. 97 che fissa i **principi di imparzialità e buon andamento dell'attività amministrativa**; l'art. 111 che stabilisce il diritto al giusto procedimento; l'art. 24 che consacra il diritto di difesa in ogni stato e grado del procedimento.

In ossequio ai suddetti parametri costituzionali, il Legislatore ha espressamente sostenuto che «l'accesso ai documenti amministrativi, attese le sue rilevanti finalità di pubblico interesse, costituisce principio generale dell'attività amministrativa al fine di favorire la partecipazione e di assicurarne l'imparzialità e la trasparenza, ed attiene ai livelli essenziali delle prestazioni concernenti i diritti civili e sociali che devono essere garantiti su tutto il territorio nazionale ai sensi dell'art. 117, secondo comma, lettera m), della Costituzione. Resta ferma la potestà delle regioni e degli enti locali, nell'ambito delle rispettive competenze, di garantire livelli ulteriori di tutela» (art. 22, comma 2, della Legge, come novellato dalla Legge 15/2005).

Da tale disposizione si evince espressamente la qualificazione ed il riconoscimento del diritto di accesso quale principio generale dell'attività amministrativa. Ma vi è di più. Dal disposto di cui all'ultimo periodo del suddetto comma si ricava, a contrario, che i

principi contenuti nell'attuale formulazione della Legge devono essere considerati come una **normativa “minima”** e, in tal senso, vincolante in ogni sua parte su tutto il territorio nazionale (OLIVERI). Infatti, alle regioni ed agli enti locali è data esclusivamente la facoltà di prevedere forme ulteriori di tutela del diritto di accesso, in senso, perciò, migliorativo rispetto alle prescrizioni minime ed inderogabili contenute nella Legge.

13.1 IL CONTENUTO DEL DIRITTO DI ACCESSO

Nella formulazione precedente alla novella del 2005, l'art. 22 della Legge non definiva espressamente il diritto di accesso, limitandosi ad evidenziarne le finalità principali: «Al fine di assicurare la trasparenza dell'attività amministrativa e di favorirne lo svolgimento imparziale è riconosciuto a chiunque vi abbia interesse per la tutela di situazioni giuridicamente rilevanti il diritto di accesso ai documenti amministrativi, secondo le modalità stabilite dalla presente legge».

Attualmente, invece, l'art. 22, primo comma, definisce il contenuto essenziale di tale diritto che consiste, appunto, nel «diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi». Tale breve definizione permette di individuare chiaramente due aspetti di fondamentale importanza per comprendere correttamente l'ambito di applicazione e di legittimazione soggettiva del diritto in questione.

Innanzitutto, **il diritto di accesso non è riconosciuto a chiunque** indistintamente, bensì soltanto agli “interessati”, ossia a quei soggetti che siano in grado di vantare un **interesse qualificato**, come previsto dal medesimo art. 22, comma 1, lettera b), in base al quale deve trattarsi di soggetti «portatori di interessi pubblici o diffusi, che

abbiano un interesse diretto, concreto ed attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso». Si evince subito chiaramente la maggiore definizione del contenuto dell'interesse giuridicamente rilevante ai fini dell'esercizio del diritto di accesso rispetto alla formulazione precedente dell'art. 22, in relazione alla quale era sufficiente dimostrare la sussistenza di un interesse connesso alla tutela di una situazione giuridicamente rilevante capace di produrre effetti, diretti o indiretti nei confronti dell'istante, a prescindere da una lesione concreta ed attuale della sua posizione giuridica e indipendentemente dal collegamento della medesima posizione al documento per il quale era chiesto l'accesso.

È evidente, dunque, la volontà del legislatore di ancorare l'esercizio di tale diritto all'esistenza effettiva di un interesse connotato di tutti gli aspetti sopra descritti, che sia funzionale a limitare condotte indiscriminate e ingiustificate dirette a porre in essere forme di controllo generalizzato dell'attività amministrativa (come, peraltro, espressamente sancito dal novellato art. 24, comma 3, della Legge).

È importante chiarire, altresì, che il diritto di accesso è riconosciuto sia nel corso del procedimento (**endoprocedimentale**) che al di fuori di esso (**esoprocedimentale**) (OLIVERI).

Nel primo caso, viene in evidenza la natura partecipativa del diritto di accesso, che consente, cioè, la partecipazione del cittadino al procedimento amministrativo in corso al fine di influenzare l'attività dell'Amministrazione. Nel secondo caso, la possibilità di esercizio del diritto di accesso successivamente alla conclusione del procedimento è correlata ai canoni costituzionali di imparzialità e trasparenza dell'agire pubblico.

In entrambi i casi, tuttavia, è necessario che l'accesso sia funzionale al soddisfacimento di un interesse diretto, concreto ed attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento indicato nell'istanza. Tale requisito, tra l'altro, si ricollega all'obbligo di motivazione della richiesta di accesso (v. art. 25, comma 2, della Legge), dalla quale deve potersi evincere con sufficiente determinatezza l'interesse sotteso all'istanza, onde consentire all'Amministrazione interessata di verificare l'effettiva legittimazione del richiedente.

13.2 ESERCIZIO DEL DIRITTO DI ACCESSO E LIMITI

Le modalità di esercizio del diritto di accesso sono attualmente disciplinate dal D.P.R. 12 aprile 2006 n. 184 “Regolamento recante disciplina in materia di accesso ai documenti amministrativi”.

L’approvazione di tale regolamento, che abroga espressamente la disciplina contenuta nel D.P.R. 27 giugno 1992 n. 352, si è resa necessaria a seguito delle rilevanti modifiche ed integrazioni recentemente apportate sul testo della legge 241/90, generando esigenze di adeguamento ed omogeneizzazione della disciplina sostanziale e procedurale vigente in materia.

Le modalità per effettuare l’accesso variano a seconda della presenza o meno di soggetti controinteressati, come individuati ai sensi dell’articolo 3 del D.P.R. 184/2006. In particolare, nel primo caso (c.d. **accesso “informale”**) sarà possibile seguire una procedura più snella ed immediata, secondo quanto previsto all’art. 5 del decreto; nel secondo caso, sarà necessario osservare prescrizioni più articolate e garantiste, rispettando quanto descritto all’art. 6 del medesimo decreto (c.d. **accesso “formale”**).

Nell’ambito del procedimento di accesso formale, è espressamente prevista la figura del “Responsabile del procedimento di accesso”, identificato nel dirigente o funzionario preposto

all'unità organizzativa ovvero in altro dipendente addetto all'unità competente a formare il documento o a detenerlo stabilmente (art. 6, comma 6, D.P.R. 184/2006). Tale previsione deve ritenersi sostanzialmente correlata a quanto disposto dagli articoli 5 e 6 della Legge in relazione alla figura ed ai compiti del Responsabile del procedimento.

Per quanto concerne l'oggetto dell'accesso, questo si esercita nei confronti di documenti amministrativi «materialmente esistenti al momento della richiesta e detenuti alla stessa data da una pubblica amministrazione, di cui all'art. 22, comma 1, lettera e), della legge, nei confronti dell'autorità competente a formare l'atto conclusivo o a detenerlo stabilmente» (art. 2, comma 2, D.P.R. 184/2006).

La Legge definisce espressamente (art. 22, comma 1, lettera d), il “documento amministrativo” come «ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale».

Con riguardo all'ambito oggettivo del diritto di accesso, è interessante quanto ha sostenuto il Consiglio di Stato in una recente sentenza:

La Sezione ritiene di non doversi discostare dal già espresso orientamento, secondo cui l'attività amministrativa, cui gli art. 22 e 23 l. n. 241 del 1990 correlano il diritto d'accesso, ricomprende non solo quella di diritto amministrativo, ma anche quella di diritto privato posta in essere dai soggetti gestori di pubblici servizi che, pur non costituendo direttamente gestione del servizio stesso, sia collegata a quest'ultima da un nesso di strumentalità derivante anche, sul versante soggettivo, dalla intensa conformazione pubblicistica (Cons. Stato, VI, n. 4152/2002; n. 2855/2002; n. 67/2002; n. 654/2001). Con alcune delle citate decisioni, la Sezione ha ritenuto che i dipendenti di P.I. s.p.a., anche cessati dal rapporto, avessero diritto ad accedere ad alcuni atti relativi all'organizzazione interna della società, quali gli atti di un procedimento privatistico per la selezione dei dirigenti o i fogli firma delle presenze giornaliera, a nulla rilevando che l'attività di Poste si svolga in parte in regime di concorrenza. In tali casi l'attività di P.I., relativa alla gestione del rapporto di lavoro con i propri dipendenti, è stata ritenuta strumentale al servizio gestito da Poste ed incidente potenzialmente sulla qualità di un servizio, il cui rilievo pubblicistico va valutato tenendo conto non solo della dimensione oggettiva, ma anche di quella propriamente soggettiva di P.I.

(Cons. Stato, sez. VI, 26.1.06, n. 229)

Con particolare riferimento alla natura documentale del provvedimento amministrativo cui si riferisce l'accesso, il Consiglio di Stato ha chiarito che:

L'accesso disciplinato dal capo V della legge n. 241/1990 ha, invero, ad oggetto i documenti amministrativi, nelle tipologie indicate dall'art. 22, comma secondo, e cioè gli atti detenuti dall'Amministrazione nella loro materialità che identificano statuizioni, accertamenti, intendimenti, pareri, volizioni, valutazioni, ecc degli organi pubblici. Non è quindi riconducibile nell'area precettiva della norma l'accesso c.d. informativo, che introduce a carico dell' Amministrazione un'attività di cognizione e di giudizio non ancora tradotta nello strumento documentale. Da ultimo si è al riguardo espressa la novella introdotta dall'art. 25 della legge 11.02.2005, n. 15, che ha dichiarato non "accessibili le informazioni in possesso di una pubblica amministrazione che non abbiano forma di documento amministrativo".

(Cons. Stato, sez. VI, 21.9.05, n. 4929)

Inoltre, il comma 3 dell'art. 22 afferma che tutti i documenti amministrativi sono accessibili «ad eccezione di quelli indicati all'articolo 24, commi 1, 2, 3, 5 e 6».

Si tratta dei casi in cui la Legge prevede espressamente l'esclusione del diritto di accesso (segreto di stato, procedimenti tributari, atti normativi e provvedimenti amministrativi generali,

procedimenti selettivi), ferma restando la potestà delle singole amministrazioni di individuare specifiche categorie di documenti, da esse formati o comunque rientranti nella loro disponibilità, sottratti all'accesso.

I casi di esclusione del diritto di accesso sono, in ogni caso, concepiti dal Legislatore come ipotesi eccezionali.

In questo senso depongono sia la *ratio* complessiva che ispira l'intera disciplina alla luce dei richiamati principi costituzionali di imparzialità, buon andamento e trasparenza dell'attività amministrativa, sia il disposto di alcune specifiche norme contenute nella Legge.

Oltre alle ipotesi sopra indicate di cui all'art. 24, commi 1, 2, 3, 5 e 6 della Legge, costituiscono ulteriori ipotesi di esclusione del diritto di accesso quelle previste:

- all'art. 22, comma 4, ai sensi del quale «Non sono accessibili le informazioni in possesso di una pubblica amministrazione che non abbiano forma di documento amministrativo, salvo quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, in materia di accesso a dati personali da parte della persona cui i dati si riferiscono»;

- all'art. 24, comma 7, per il quale «Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici. Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale».

L'art. 24, comma 4, contiene una norma di indirizzo in base alla quale l'accesso ai documenti amministrativi non può essere negato «ove sia sufficiente fare ricorso al potere di differimento». Tale disposto normativo conferma la volontà del Legislatore di limitare al massimo le ipotesi di esclusione, prevedendo che, ove possibile, l'Amministrazione faccia ricorso al differimento. Resta salvo che il provvedimento mediante il quale l'Amministrazione disporrà il differimento dovrà indicarne espressamente la durata ed essere supportato da adeguate motivazioni, in quanto il differire l'esercizio del diritto rappresenta pur sempre, se non una negazione, certamente una limitazione, anche se solo temporale, del diritto stesso (v. art. 9, comma 2, D.P.R. 184/2006; art. 25, comma 3, della Legge).

È interessante far notare, infine, che il legislatore ha voluto dare pieno riconoscimento, anche in tale settore, all'uso delle nuove tecnologie informatiche. Tale volontà deve ritenersi funzionale alla rimozione di qualunque ostacolo, giuridico e non, all'esercizio del diritto di accesso, nei casi e nei limiti previsti per legge.

In questo senso, deve essere vista con estremo favore la disposizione di cui all'art. 13 D.P.R. 184/2006 che disciplina, appunto, l'accesso per via telematica: «Le pubbliche amministrazioni di cui all'articolo 22, comma 1, lettera e), della legge, assicurano che il diritto d'accesso possa essere esercitato anche in via telematica. Le modalità di invio delle domande e le relative sottoscrizioni sono disciplinate dall'articolo 38 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni, dagli articoli 4 e 5 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, e dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni».

13.3 DIRITTO DI ACCESSO E PRIVACY

La disciplina del diritto di accesso presenta aspetti ed implica valutazioni che non possono prescindere da un coordinamento con la normativa in materia di tutela dei dati personali.

Lo ha ben compreso il legislatore il quale, nel novellare la legge 241/90, ha inserito nel corpo della stessa alcuni riferimenti e rinvii al Codice in materia di trattamento dei dati personali (d.lgs. 30 giugno 2003, n. 196). A sua volta, l'art. 59 del d.lgs. 196/2003 contiene un rinvio generale in materia di accesso concernente dati personali alla disciplina contenuta nella legge 241/90 e nei relativi regolamenti di attuazione.

Ai sensi dell'art. 24, comma 7, della Legge, qualora l'istanza di accesso concerna documenti contenenti dati sensibili e giudiziari, l'esercizio del diritto di accesso è consentito «nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale».

In particolare, l'art. 60 del d.lgs. 196/2003 stabilisce che, se il trattamento riguarda dati idonei a rivelare lo stato di salute o la vita sessuale, lo stesso è ammesso nei limiti in cui «la situazione giuridicamente rilevante che si intende tutelare con la richiesta di

accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile».

Affinché il diritto di accesso prevalga sul diritto alla riservatezza è, dunque, necessario che il diritto sotteso all'istanza abbia un peso, un valore tale da implicare una tutela giuridica di forza non inferiore a quella prevista dall'ordinamento a salvaguardia dei diritti del titolare dei dati stessi.

Tale principio era pacifico in giurisprudenza già in epoca precedente all'entrata in vigore del d.lgs. 196/2003. Si veda, in tal senso, quanto sostenuto dal T.A.R. Lazio Latina, nella sentenza del 15 novembre 2002, n. 1179, secondo il quale la ponderazione comparativa tra il diritto di accesso e quello alla riservatezza - da effettuarsi in concreto, in primo luogo, dall'amministrazione ed eventualmente, in sede di controllo, dal giudice amministrativo adito ai sensi dell'art. 25 della legge 241/90 - può comportare che il diritto posto a base della richiesta di accesso, pur se astrattamente di rango inferiore rispetto a quello alla riservatezza, risulti in concreto prevalente su quest'ultimo, in considerazione del grado minimo di effettivo rilievo della dignità e della privacy dell'interessato.

Di recente, è intervenuto il Consiglio di Stato ritenendo che:

...l'interesse alla riservatezza, tutelato dalla normativa mediante una limitazione del diritto di accesso (art. 24, comma 2, lett. d, della l. n. 241/1990 e art. 8, comma 5, lett. d, del d.p.r. n. 352/1992), deve considerarsi recessivo quando l'accesso stesso sia esercitato, come nella fattispecie in esame, per la difesa di un interesse giuridico, nei limiti in cui esso è necessario alla difesa di quell'interesse .

(Cons. Stato, sez. VI, 20.4.06, n. 2223).

Nello stesso senso, si era già pronunciato il Consiglio di Stato, sez. VI, con sentenza 22.11.05, n. 6524. Successivamente anche il T.A.R. sez. I Calabria - Reggio Calabria - 3.12.05, n. 2179 giunge ad affermare che il bilanciamento di interessi comporta che il diritto di accesso ai documenti amministrativi prevale sull'esigenza di riservatezza del terzo ogniqualvolta l'accesso venga in rilievo per la cura o la difesa di interessi giuridici del richiedente, salvo che non si tratti di dati personali (dati c.d. sensibili) nel qual caso l'art. 16, secondo comma, d.lgs. 11.5.99 n. 135 (ora art. 60 del d.lgs. n. 196 del 2003) prescrive che l'accesso sia possibile solo se il diritto che il richiedente deve far valere o difendere è di rango almeno pari a quello della persona cui si riferiscono i dati stessi.

Un'altra disposizione della Legge che si caratterizza per il suo coordinamento sostanziale con le finalità sottese alla normativa in materia di tutela dei dati personali è quella contenuta all'art. 22, comma 4, in base al quale: «Non sono accessibili le informazioni in possesso di una pubblica amministrazione che non abbiano forma di documento amministrativo, salvo quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, in materia di accesso a dati personali da parte della persona cui i dati si riferiscono».

Tale norma riconosce espressamente un diritto insopprimibile che spetta esclusivamente al soggetto cui si riferiscono i dati in possesso dell'Amministrazione, relativamente ai quali l'interessato propone l'istanza di accesso. Nessuna limitazione può incontrare, in tali ipotesi, la richiesta di accesso anche qualora tali dati non siano contenuti in documenti propriamente amministrativi (ai sensi dell'art. 22, comma 1, lettera d).

Ciò in considerazione del combinato disposto tra tale disposizione e l'art. 7 del d.lgs. 196/2003 ai sensi del quale l'interessato ha diritto di opporsi, in tutto o in parte, al trattamento, nonché di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile, ed altresì di chiedere l'aggiornamento, la rettificazione, la cancellazione o l'integrazione dei dati stessi.

Qualora, invece, la richiesta di accesso concerna un documento dal quale si evincano dati personali non riferibili al soggetto istante bensì a terzi, il diritto di accesso è soggetto al trattamento previsto dal d.lgs. 30 giugno 2003, n. 196.

In questo senso, se l'Amministrazione cui è pervenuta l'istanza di accesso individua soggetti "controinteressati" è tenuta a darne comunicazione agli stessi, mediante invio di copia con raccomandata con avviso di ricevimento, o per via telematica (v. art. 3 del D.P.R. 184/2006).

Entro il termine di dieci giorni dal ricevimento della suddetta comunicazione, i soggetti controinteressati potranno presentare motivata opposizione alla richiesta di accesso. Decorso invano tale termine, l'Amministrazione potrà provvedere in merito alla richiesta.

La definizione di soggetti "controinteressati" è espressamente contenuta all'art. 22, comma 1, lettera c), della Legge, ai sensi del quale si intendono «per "controinteressati", tutti i soggetti, individuati o facilmente individuabili in base alla natura del documento richiesto, che dall'esercizio dell'accesso vedrebbero compromesso il loro diritto alla riservatezza».

L'art. 3 del D.P.R. 184/2006 aggiunge, peraltro, che l'Amministrazione, nell'individuare la presenza di eventuali soggetti controinteressati, debba tenere conto altresì del contenuto degli "atti

connessi”, come definiti all’art. 7, comma 2, del medesimo decreto. Tale ultima disposizione prevede che l'accoglimento della richiesta di accesso a un determinato documento amministrativo implica anche la facoltà di accesso agli altri documenti nello stesso richiamati e appartenenti al medesimo procedimento, fatte salve le eccezioni di legge o di regolamento.

Tale previsione deve ritenersi fondata sulla volontà di far sì che il riconoscimento del diritto di accesso non sia solo formale, bensì sostanziale. In questo senso, un accesso limitato al documento specifico indicato dall’interessato nella richiesta realizzerebbe, di fatto, un accesso parziale, in quanto è evidente che il contenuto di un determinato documento è pienamente intelligibile soltanto se letto in relazione agli eventuali ulteriori documenti nello stesso richiamati ovvero con esso connessi e/o collegati.

13.4 DIRITTO DI ACCESSO E RICORSI

L'art. 25 della Legge disciplina le modalità attraverso cui l'interessato può proporre ricorso contro le determinazioni amministrative concernenti il diritto di accesso.

In particolare, il comma 4 di tale articolo stabilisce che, in caso di diniego dell'accesso, espresso o tacito, ovvero di differimento dello stesso ai sensi dell'art. 24, comma 4, della Legge, il richiedente ha la possibilità:

- 1) di proporre ricorso, entro trenta giorni, al tribunale amministrativo regionale ai sensi del comma 5 dell'art. 25 della Legge;
- 2) chiedere, entro trenta giorni e soltanto nei confronti degli atti delle amministrazioni comunali, provinciali e regionali, al Difensore civico territorialmente competente, che sia riesaminata la suddetta determinazione;
- 3) presentare, nei confronti di atti delle amministrazioni centrali o periferiche dello Stato, la medesima richiesta di cui al punto precedente alla Commissione per l'accesso disciplinata all'art. 27 della Legge.

Nel primo caso, si tratta di un rimedio giurisdizionale di carattere generale offerto al cittadino contro le determinazioni della Pubblica

amministrazione in materia di accesso alla documentazione amministrativa.

Il Consiglio di Stato pronunciandosi sulla questione se sia ammissibile o meno il ricorso nella specie proposto ai sensi dell'art. 25 della Legge e non notificato all'unico controinteressato ha ritenuto che

...il giudizio previsto dall'art.25 cit., salve le deroghe da esso espressamente previste, va sottoposto alla generale disciplina del processo amministrativo e che, tra i relativi principi, vi sia anche quello sancito all'art.21, comma 1, L. n.1034/1971, per il quale il ricorso deve essere notificato tanto all'organo che ha emanato l'atto "quanto ai controinteressati ai quali l'atto direttamente si riferisce, o almeno ad uno di essi", regola questa che è coerente con il giudizio sull'accesso e con la posizione giuridica fatta valere col ricorso ex art.25 L. n.241/1990.

(Consiglio di Stato, sez. VI, 31.5.06, n. 3323)

Deve ritenersi, invece, che gli strumenti previsti ai precedenti punti 2 e 3 rappresentino rimedi utilizzabili soltanto in relazione alle specifiche condizioni e categorie di atti espressamente indicati.

Nell'ambito della disciplina dettata per tali ipotesi dall'art. 25, comma 4, della Legge è altresì previsto che: «Se l'accesso è negato o differito per motivi inerenti ai dati personali che si riferiscono a soggetti terzi, la Commissione provvede, sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta, decorso inutilmente il quale il parere si intende reso».

Lo stesso comma, novellato da ultimo dalla Legge 15/2005, ha previsto inoltre che: «Qualora un procedimento di cui alla sezione III del capo I del titolo I della parte III del decreto legislativo 30 giugno 2003, n. 196, o di cui agli articoli 154, 157, 158, 159 e 160 del medesimo decreto legislativo n. 196 del 2003, relativo al trattamento pubblico di dati personali da parte di una pubblica amministrazione, interessi l'accesso ai documenti amministrativi, il Garante per la protezione dei dati personali chiede il parere, obbligatorio e non vincolante, della Commissione per l'accesso ai documenti amministrativi. La richiesta di parere sospende il termine per la pronuncia del Garante sino all'acquisizione del parere, e comunque per non oltre quindici giorni. Decorso inutilmente detto termine, il Garante adotta la propria decisione».

Si tratta delle ipotesi in cui l'interessato sceglie di ricorrere al Garante in alternativa all'autorità giudiziaria (artt. 145-151 d.lgs.

196/2003), ovvero dei casi in cui il Garante, per l'espletamento dei propri compiti, disponga accertamenti, verifiche o controlli (artt. 157-160 d.lgs. 196/2003).

*13.5 IL DIRITTO DI ACCESSO TRA IL CODICE PER LA
PROTEZIONE DEI DATI PERSONALI E IL CODICE
DELL'AMMINISTRAZIONE DIGITALE.*

L'introduzione da parte del Codice dell'amministrazione digitale (d.lgs. 7.3.05, n. 82) del diritto di richiedere ed ottenere l'uso delle nuove tecnologie della comunicazione da parte della Pubblica Amministrazione determina il sorgere di una nuova dimensione dei rapporti tra Stato e cittadino. Dall'affermazione del suddetto principio deriva anche e soprattutto il diritto alla partecipazione al procedimento amministrativo informatico (BERTONI). L' art. 4 del C.A.D., infatti, sancisce che «la partecipazione al procedimento e il diritto di accesso ai documenti amministrativi sono esercitabili mediante l'uso delle tecnologie dell'informazione e della comunicazione secondo quanto disposto dagli articoli 59 e 60 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. Ogni atto e documento può essere trasmesso alle pubbliche amministrazioni con l'uso delle tecnologie dell'informazione e della comunicazione se formato ed inviato nel rispetto della vigente normativa». L'art. 41, secondo comma, del C.A.D. in piena sintonia con quanto affermato dispone che la Pubblica Amministrazione titolare del procedimento possa raccogliere in un fascicolo informatico gli atti e i dati del procedimento medesimo da chiunque

formati. Tale procedura dovrà garantire l'esercizio in via telematica dei diritti previsti dalla legge 241 del 1990. I dati delle pubbliche amministrazioni, quindi, devono essere resi disponibili ed accessibili con l'uso delle nuove tecnologie informatiche in modo da consentirne la fruizione alle condizioni fissate dall'ordinamento dalla stessa Pubblica Amministrazione e dai privati (art. 50 C.A.D.). Tuttavia, l'amministrazione, titolare dei dati, dovrà garantire nell'ambito di tale disponibilità ed accesso il rispetto dei limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti e in particolare la protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico. Il presupposto per tale interscambio di dati ed informazioni tra pubbliche amministrazioni rimane comunque il principio della necessità del trattamento dei dati personali e di pertinenza e non eccedenza dei dati trattati. Il fatto di poter accedere a tutto non giustifica il fatto di accedervi concretamente al di fuori un reale e motivato interesse della Pubblica Amministrazione. Per questo motivo devono essere predisposti dei meccanismi atti a controllare e tutelare i dati personali custoditi negli archivi (ormai globali ed interattivi) contro gli accessi non autorizzati non solo provenienti dall'esterno ma anche e soprattutto dalle stesse Pubbliche Amministrazioni.

BIBLIOGRAFIA GENERALE

CASSESE, *Istituzioni di diritto amministrativo*, Milano, 2004.

GIACOPUNZI-LISI, *Guida al Codice dell'amministrazione digitale*, Matelica (MC), 2006.

BALDASSARE, *Privacy e Costituzione*, Roma 1974

BRANDEIS L.D. E WARREN S.D., *The right to privacy*, in *Harvard Law Review*, 1890, 193-220.

CERULLI IRELLI, *Corso di Diritto Amministrativo*, Torino.

D'ATENA, *Lezioni Tematiche di Diritto Costituzionale*, Roma, 1996, 222.

GERMANI, *origini ed evoluzione del concetto di privacy nell'esperienza di common law*, in *Giur. di Merito*, 1975, 152

GRIPPO, *Intenert e dati personali*, in *Privacy*, in *Enc. Cendon*, Padova, 1999, 284.

LATTANZI, *Dati sensibili: una categoria problematica nell'orizzonte europeo*, in *Europa e Diritto Privato*, 1998.

MACCABONI, *La profilazione dell'utente telematico fra tecniche pubblicitarie online e tutela della privacy*, in *Il diritto dell'informazione e dell'informatica*, 2001, 425.

MANCINI, *La tutela dei diritti dell'uomo: il ruolo della Corte di Giustizia delle Comunità europee*, in *Riv. Trim. dir. proc. civ.* 1989.

- MONDUCCI, *Il trattamento dei dati personali nei contratti on line*, in *Diritto delle nuove tecnologie informatiche e dell'internet* (a cura di GIUSEPPE CASSANO), IPSOA, 2002.
- PAGANELLI, *Diritti della personalità. L'individuo e il gruppo*, in *Diritto privato europeo* (a cura di LIPARI), Padova, 1997
- PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, 2002,12.
- PARODI-CALICE, *Responsabilità penali e Internet*, Milano, 2001.
- RODOTÀ, *Tecnologie e diritti*, Bologna, 1995.
- SAMARAJIVA, *Interactivity as though privacy matterei*, in AGRE – ROTEMBERG, *Technology and Privacy: The new Landscape*, Massachusetts, 1997, 277.
- SATTA, *Giustizia amministrativa*, Padova, 1997
- SATTA, *Imparzialità della pubblica amministrazione*, in *Enc. Giuridica*, XV, Roma, 1988.
- SATTA, voce *Atto amministrativo*, in *Enc. Giur.*, IV, 1989
- SCALISI, *Il diritto alla riservatezza*, Milano, 2002, 307
- STILO, *Il documento elettronico nella società dell'informazione*, in *Il Nuovo Diritto*, n. 9, 2004.
- STILO, *La fine di una spontanea confidenzialità delle comunicazioni*, in *Il Nuovo Diritto*, n. 9-10, 2006.

STILO, *La Nuova Era Digitale tra vecchie e nuove storie*, in *Il Nuovo Diritto* n. 11, 2002, pag. 69.

STILO, *Sicurezza e dato informatico: spunti per una teoria generale del diritto della sicurezza informatica*, in *Il Nuovo Diritto*, n. 11, 2002, 76.

STILO, *Sicurezza e dato informatico: spunti per una teoria generale del diritto della sicurezza informatica*”, in *Il Nuovo Diritto* n. 11, 2002, pag. 76.

STILO, *La pubblica amministrazione tra diritto di accesso e trattamento dei dati personali*, in *Il Nuovo Diritto*, n.12, 2006, 1135.

OLIVIERI, *La riforma della legge sul procedimento amministrativo: profili attuativi ed applicativi*, Matelica (MC), 2006.

TESAURO, *I principi fondamentali nella giurisprudenza della Corte di Giustizia*, in *Riv. Internaz. diritti dell'uomo*, 1992.

WACKS, *Personal Information. Privacy and the Law*, Oxford, 1993.

LISI – BERTONI, *Pubblica Amministrazione e privacy*, Roma, 2006.

DI MARTINO – VOLTAN, *Diritto della privacy per le imprese e i professionisti*, Forlì, 2006.

GIURDANELLA – GUARNACCIA, *Elementi di diritto amministrativo elettronico*, Matelica (MC), 2005

BORRUSO, *La tutela del documento e dei dati* in AA.VV., *Profili penali dell'informatica*, 1994.

DI RAGO, *La privacy e le imprese*, Matelica (MC), 2005

INDICE ANALITICO

(I NUMERI SI RIFERISCONO AI CAPITOLI E PARAGRAFI)

- innovazione, 1
- accesso ai dati personali, 13
- Codice dell'amministrazione digitale e privacy, 13.5
- Codice in materia di protezione dei dati personali, 5
- Convenzione di Strasburgo, 5
- dati giudiziari,6
- dati sensibili, 6
- gestione dei dati personali, 2
- incaricato del trattamento,8
- interessato (i diritti), 9
- regole ulteriori per la P.A., 11
- responsabile del trattamento, 8
- responsabilità e struttura piramidale, 8
- sicurezza e misure minime, 12
- titolare del trattamento, 8
- trattamento dei dati personali e diritti fondamentali, 4
- trattamento illecito (le responsabilità), 10
- dati biometrici, 6
- dati personali, 6

-diritto di accesso e ricorsi, 13.4

-organigramma privacy, 8



TUTTI I DIRITTI RISERVATI