Consiglio Nazionale delle Ricerche

Istituto di Scienza e Tecnologie dell'Informazione
"A. Faedo"

Sicurezza dei Dati

e

Applicazione del Codice della Privacy

(D.L.gs 196/2003)

Rosaria Deluca

Sommario

INTRODUZIONE

Il Decreto legislativo 30 giugno 2003, entrato in vigore dal 1 gennaio 2004, è nato dall'esigenza di uniformare le leggi emanate fino ad oggi in materia di protezione dei dati personali in modo da offrire un materiale normativo più organico ed equilibrato, più rispettoso dei diritti del cittadino, più in linea con lo sviluppo delle tecnologie, più capace di valorizzare la partecipazione dei gruppi sociali all'attuazione delle norme.

Esso riunisce in unico contesto la legge 675/1996 e gli altri decreti legislativi, regolamenti e codici deontologici che si sono succeduti in questi anni e contiene anche importanti innovazioni tenendo conto della "Giurisprudenza" del Garante e della direttiva Ue 2000/58 sulla riservatezza nelle comunicazioni elettroniche. Il presente "Testo Unico" nell'art. 2 comma 1 è denominato Codice. E' importante ricordare che i Testi Unici, per loro natura, costituiscono lo strumento primario della semplificazione amministrativa che ha caratterizzato gli ultimi dieci anni, nell'ambito del diritto pubblico. Il Codice infatti è proprio l'espressione dell'esigenza di semplificazione di un corpo normativo contenente norme talvolta oscure o persino contraddittorie.

In questo lavoro è stata effettuata un'analisi dettagliata degli aspetti fondamentali del Testo Unico in modo da fornire uno strumento adeguato di lettura per una corretta conoscenza e comprensione della normativa vigente in relazione ai principi che la regolano, ai diritti, agli adempimenti, alle sanzioni.

In particolare gli obiettivi sono stati i seguenti:

- fornire le conoscenze di base relative al tema del trattamento dati
- comprendere i ruoli e le responsabilità nel sistema di gestione della sicurezza dei dati
- acquisire e diffondere, nella struttura di appartenenza, la cultura della riservatezza e della tutela dei dati personali

1 FONTI NORMATIVE: DALLA NORMATIVA EUROPEA AI PRINCIPI GENERALI DEL CODICE

1.1 La normativa Europea

L'Art. 8 della Convenzione Europea dei Diritti dell'Uomo del 1950, elaborata all'indomani del secondo conflitto mondiale, riconosce tra i diritti fondamentali dell'uomo quello al rispetto della vita privata e familiare, del proprio domicilio e della propria corrispondenza. Tale garanzia è stata ampliata dalla Carta dei Diritti fondamentali dell'Unione Europea, del 2000, agli articoli 7 e 8.

L'art. 8, in particolare stabilisce che "Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

Successivamente la Bozza della Convenzione Europea approvata il 18 luglio 2003 stabiliva che "Ogni individuo ha diritto alla protezione dei dati personali che lo riguardano e inoltre ribadiva che "La Legge Europea stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e delle agenzie dell'Unione, e da parte degli stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione dei dati. Il rispetto di tali norme è soggetto al controllo di un'autorità indipendente."

Il "diritto ad essere lasciato solo" (il cd. Right to be alone), tipico dei paesi anglosassoni, concepito quale fondamentale diritto alla propria riservatezza dalle aggressioni dei mass media, ha lasciato oggi spazio ad una nozione più ampia del diritto alla propria privacy.

Oggi la privacy, dovendo fare i conti con la società dell'informazione,"dove è impossibile transitare senza lasciare tracce"(*R. Acciai, ex-Garante Privacy)*, da strumento passivo di difesa dalle intrusioni altrui, è divenuta strumento di libertà e partecipazione e, quindi, potere di controllo e conoscenza sulla circolazione dei propri dati personali.

Il diritto alla protezione dei dati personali non è più, quindi, un diritto elitario collegato alla notorietà, ma si è sviluppato e costituzionalizzato quale nuovo diritto del cittadino.

L'importanza rivestita dalla privacy ha portato nel tempo a direttive europee e di conseguenza, alle successive leggi nazionali di recepimento, fino al formarsi di un apposito tessuto normativo frutto dello stratificarsi dei numerosi interventi legislativi.

1.2 L'ordinamento costituzionale italiano

Nel nostro ordinamento non esistono fonti normative precedenti il Codice che esprimano tutela alla riservatezza. Per contro la Carta Costituzionale riconosce espressamente alcune libertà che potrebbero atteggiarsi al limite della riservatezza.

Art. 2 "*La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale".*

Art. 3 "*Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali".*
"È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'uguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese".

E' controversa l'interpretazione sulla natura di clausola generale dell'art. 2 Cost. e sulla la dimensione individuale o sociale dell'art.3 Cost. (L'art. 2 ha natura di clausola generale?….L'art.3 va letto in una dimensione individuale o sociale?)

Art.13 "*La libertà personale è inviolabile".*
"Non è ammessa forma alcuna di detenzione, di ispezione o perquisizione personale, né qualsiasi altra restrizione della libertà personale, se non per atto motivato dell'autorità giudiziaria e nei soli casi e modi previsti dalla legge".
"In casi eccezionali di necessità ed urgenza, indicati tassativamente dalla legge, l'autorità di pubblica sicurezza può adottare provvedimenti provvisori, che devono essere comunicati entro quarantotto ore all'autorità giudiziaria e, se questa non li convalida nelle successive quarantotto ore, si intendono revocati e restano privi di ogni effetto".
È punita ogni violenza fisica e morale sulle persone comunque sottoposte a restrizioni di libertà.
"La legge stabilisce i limiti massimi della carcerazione preventiva".

Art. 14 *"Il domicilio è inviolabile".*
Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale.
Gli accertamenti e le ispezioni per motivi di sanità e di incolumità pubblica o a fini economici e fiscali sono regolati da leggi speciali.

Art. 15 *"La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili".*
"La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge".

Queste norme sanciscono l'inviolabilità della libertà personale, del domicilio, della libertà e segretezza della corrispondenza e ogni altra forma di comunicazione.
La libertà personale viene intesa non solo in senso fisico, ma con riguardo alla persona nella sua interezza, compresa la sfera spirituale e la sua personalità.
In questo caso domicilio e corrispondenza sono interpretati come proiezione spaziale e spirituale dell'individuo.
La maggior parte della dottrina esprime sfavore verso l'utilizzo di queste norme come fondamento costituzionale per il diritto alla riservatezza.

Art. 21 *"Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione".*
"La stampa non può essere soggetta ad autorizzazioni o censure".
"Si può procedere a sequestro soltanto per atto motivato dell'autorità giudiziaria nel caso di delitti, per i quali la legge sulla stampa espressamente lo autorizzi, o nel caso di violazione delle norme che la legge stessa prescriva per l'indicazione dei Responsabili".
"In tali casi, quando vi sia assoluta urgenza e non sia possibile il tempestivo intervento dell'autorità giudiziaria, il sequestro della stampa periodica può essere eseguito da ufficiali di polizia giudiziaria, che devono immediatamente, e non mai oltre ventiquattro ore, fare denunzia all'autorità giudiziaria. Se questa non lo convalida nelle ventiquattro ore successive, il sequestro s'intende revocato e privo di ogni effetto".

"La legge può stabilire, con norme di carattere generale, che siano resi noti i mezzi di finanziamento della stampa periodica".
"Sono vietate le pubblicazioni a stampa, gli spettacoli e tutte le altre manifestazioni contrarie al buon costume. La legge stabilisce provvedimenti adeguati a prevenire e a reprimere le violazioni".

Si tratta di una norma "ambivalente", in parte contraddittoria, in quanto utilizzata per sancire due importanti principi:

- negare la rilevanza costituzionale del diritto alla riservatezza perché ritenuta incompatibile con la libertà di espressione
- fondare il principio costituzionale del diritto alla riservatezza proprio su questa disposizione

La giurisprudenza consolidata si fonda proprio sul criterio di bilanciamento, relativo e non assoluto, ispirato ai tre parametri dell'interesse sociale, della notizia della verità dei fatti narrati e della purezza.

Ulteriori interventi legislativi

l.n. 675/96	d.lgs n. 51/99	l. n. 127/01
l.d.n.676/96	d.lgs n. 135/99	l. n. 325/00
d.lgs n. 123/97	d.lgs n. 281/99	d.lgs. 467/01
d.lgs n. 255/97	d.lgs n. 282/99	d.p.r.n.318/99
d.lgs n. 135/98	l.n. 344/98	
d.lgs n. 389/98	l.n. 25/99	

La legge fondamentale n. 675/96 è stata più volte integrata e modificata fino al d.lgs. n. 196/03 (Codice della privacy), a sua volta ancora integrato dalla l. n. 45/04.

1.3 Aspetti generali del codice

Il Codice è diviso in tre parti:

- La prima parte è dedicata alle disposizioni generali, ordinate in modo da trattare tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato

- La seconda parte è dedicata a settore specifici. Essa, oltre a disciplinare aspetti specifici, introduce la disciplina per il settore sanitario e quella dei controlli sui lavoratori

- La terza parte affronta la materia della tutela amministrativa e giurisdizionale con il consolidamento delle sanzioni amministrative e penali e con le disposizioni sull'ufficio del Garante

2 DISPOSIZIONI GENERALI

Diritto alla protezione dei dati personali (Art.1)

Il Codice esordisce con un'affermazione di principio:
"Chiunque ha diritto alla protezione dei dati personali che lo riguardano". Non c'è dunque alcuna distinzione, almeno con riferimento all'ambito soggettivo di operatività delle norme, tra cittadini, stranieri, apolidi, persone fisiche e persone giuridiche, enti o associazioni non riconosciute ovvero dotati di personalità giuridica.

Principio di finalità (Art.2)

In base a tale principio il Codice riconosce che il trattamento dei dati personali si svolga "nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato" e garantisce l'effettività di tali diritti e di tali libertà attraverso la "semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte dei titolari del trattamento".

Principio di necessità (Art.3)

In base a tale principio i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzo di dati personali e di dati identificativi.
I dati personali devono essere trattati solo quando le finalità perseguite nei singoli casi non possono essere realizzate mediante dati anonimi o altre modalità che permettano di identificare l'interessato solo in caso di necessità.
Questa è una prescrizione che rappresenta un'autentica novità dal punto di vista normativo e che sembra aver ratificato quell'opinione dominante in dottrina secondo cui l'anonimato è uno degli strumenti più idonei a garantire la tutela della riservatezza

Si tratta di principi generali di fondamentale importanza perché costituiscono la guida interpretativa per tutte le norme contenute nel Codice.

2.1 ESPRESSIONI LETTERALI RICORRENTI NEL CODICE

Il legislatore offre una precisa descrizione delle operazioni che hanno ad oggetto dati personali ***(Art. 4)*:**

Trattamento
È qualunque operazione o insieme di operazioni, compiute anche senza il supporto di strumenti elettronici, concernenti la raccolta, 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 dati.

Dato personale
È qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione identificato o identificabili, anche in modo indiretto, mediante riferimento a qualsiasi altra informazione, compreso il numero di identificazione personale.

Dati sensibili
Sono dati personali che permettono la rivelazione dell'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.

Titolare
È 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 relative ad altre finalità, alle modalità di trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile
Figura definita dalla legge ma solo eventuale con lo scopo di supportare l'attività del titolare è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali.

Incaricati
Sono le persone fisiche autorizzate a effettuare operazioni di trattamento dal titolare o dal responsabile.

Interessato
È la persona giuridica, ente o associazione cui si riferiscono i dati personali.

Comunicazione
Consiste nel 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 agli incaricati, in qualsiasi forma, anche attraverso la loro messa a disposizione o consultazione.

Diffusione
Consiste nel dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche attraverso la loro messa a disposizione o consultazione.

Blocco
Consiste nella conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.

Garante
E' un'autorità istituita dalla legge precedente (l. n. 675/1996) per assicurare la tutela dei diritti e delle libertà fondamentali ed il rispetto della dignità nel trattamento dei dati personali.

E’ un organo collegiale, composto da quattro membri eletti dal Parlamento, con voto limitato tra persone che assicurino indipendenza e che siano esperte di riconosciuta e comprovata competenza nelle materie del diritto o dell’informatica, garantendo al contempo la presenza di entrambe le qualifiche. Come in ogni organo collegiale i componenti eleggono nel loro ambito un Presidente, il cui voto prevale in caso di parità, ed eleggono un vice-Presidente, che assume le funzioni di Presidente in caso di assenza o impedimento di quest’ultimo. Il Presidente e i componenti durano in carica quattro anni e non possono essere confermati per più di una volta. Per tutta la durata dell’incarico costoro sono soggetti a una serie di limitazioni tanto è che non possono esercitare, a pena di decadenza dalla carica di membri dell’Autority, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive. L’attuale collegio si è insediato il 18 Aprile 2005.

3 DIRITTI DELL'INTERESSATO

L'interessato ha diritto di conoscere ***(Art.7)*:**

- l'origine dei propri dati personali
- le finalità e le modalità del loro trattamento
- la logica applicata al trattamento effettuato con strumenti elettronici
- gli estremi identificativi del titolare, dei responsabili e del rappresentante designato a norma di legge, dei soggetti o delle categorie ai quali i dati personali possono essere comunicati
- ha altresì il diritto ad ottenerne la trasformazione in forma anonima ovvero ancora il blocco ovvero la conservazione del trattamento, quando esso avvenga in violazione di legge
- ha diritto, ad avere precisa e puntuale attestazione che le operazioni di aggiornamento e/o di cancellazione siano state portate a conoscenza dei soggetti ai quali i dati sono stati comunicati o diffusi, eccetto il caso in cui tale adempimento sia impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato
- l'interessato infine, ha diritto di opporsi, in tutto in parte, purché per motivi legittimi, al trattamento dei dati personali che lo riguardano ancorché pertinenti allo scopo della raccolta, e al trattamento che avvenga per fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazioni commerciali

Nessuna formalità particolare è stata prevista per l'esercizio dei diritti di cui si è detto in precedenza ***(Art.8)*.**

In particolare, ai fini dell'esercizio del diritto di accesso ai dati, l'interessato non è tenuto ad esplicitare le ragioni della sua richiesta di accesso, che può concernere soltanto le informazioni riferite alla propria persona e non può essere estesa ai dati relativi a terzi.
Tuttavia, rispetto a questo principio generale sono previste deroghe in cui i diritti previsti dall'art.7 non possono essere esercitati, né con richiesta al titolare o al responsabile, né con ricorso al Garante.

Si tratta delle ipotesi in cui il trattamento avviene conformemente alle disposizioni di legge tese a:

- reprimere il fenomeno del riciclaggio
- sostenere le vittime di richieste estorsive
- sia posto in essere da commissioni parlamentari d'inchiesta

4 REGOLE GENERALI PER IL TRATTAMENTO DEI DATI

In materia di protezione dei dati personali sono previste le seguenti regole ***(Art.11)*****:**

- liceità e correttezza
- raccolta e registrazione per scopi determinati, espliciti e legittimi
- esattezza
- pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono raccolti e registrati
- conservazione finalizzata all'identificazione dell'interessato per il periodo necessario al raggiungimento dello scopo.

Costituiscono condizione essenziale per la liceità e correttezza del trattamento dei dati personali

- il rispetto delle disposizioni contenute nei codici di deontologia e di buona condotta promossi dal Garante, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa, pubblicati nella Gazzetta Ufficiale ***(Art.12)***
- l'osservanza dei Provvedimenti del Garante ***(Art.154-160)*****.**

In caso di cessazione del trattamento i dati sono ***(Art. 16)*****:**

- distrutti
- ceduti ad altro titolare per ulteriore trattamento compatibile con gli scopi originari della raccolta
- conservati per fini personali e sottratti a comunicazione o diffusione
- conservati o ceduti ad altro titolare ai fini storici, statistici o scientifici secondo le disposizioni normative
- sono trattati in base a un obbligo previsto dalla legge
- sono trattati ai fini di investigazioni difensive

4.1 Regole ulteriori per i soggetti pubblici

Avendo il trattamento di dati da parte della pubblica amministrazione un'importanza sociale e un valore di interesse collettivo elevati, il legislatore ha, quindi, previsto una disciplina specifica e funzionale al conseguimento dell'armonia degli interessi in gioco.

4.2 Principi applicabili a tutti i tipi di trattamento

Principio di legalità (Art.18)**.**
In base a tale principio tutti i soggetti pubblici, con la sola eccezione degli enti pubblici economici, possono trattare i dati personali esclusivamente per lo svolgimento delle funzioni istituzionali alle quali sono preposti, pur dovendo sempre attenersi alle prescrizioni codicistiche vigenti in materia e nei limiti imposti dalle leggi e dai regolamenti.

Il quarto comma dell'articolo 18 dispone, inoltre, che salvo quanto previsto per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, la pubblica amministrazione può trattare dati personali, senza dover acquisire il consenso espresso dell'interessato.

4.3 Principi applicabili al trattamento dei dati diversi da quelli sensibili e giudiziari

Il trattamento da parte di un soggetto pubblico (non economico) riguardante dati diversi da quelli sensibili e giudiziari è consentito soltanto per lo svolgimento di funzioni istituzionali
Un soggetto pubblico può comunicare dati personali "comuni" ad altri soggetti pubblici, purché ciò sia previsto da una legge o regolamento. In assenza di una tale norma, la comunicazione è permessa solo se necessaria per lo svolgimento di funzioni istituzionali.
Nel caso di enti pubblici economici, la comunicazione e la diffusione sono ammesse unicamente quando sono previste da una norma di legge o di regolamento ***(Art.19)*.**

4.4 Principi applicabili al trattamento dei dati sensibili

Il trattamento dei dati sensibili da parte di soggetti pubblici (non economici) è consentito solo se autorizzato da espressa disposizione di legge, nella quale siano specificate le tipologie di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. Nei casi in cui una disposizione di legge precisi la rilevante necessità di interesse pubblico ma non menzioni le categorie di dati sensibili e le operazioni eseguibili, il trattamento è ammesso solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici con atto di natura regolamentare adottato in conformità al parere espresso del Garante (art. 154) anche sulla base di schemi-tipo.
Se invece il trattamento non è previsto espressamente da una disposizione di legge, i soggetti pubblici possono chiedere al Garante di individuare le attività, tra quelle previste dalla legge per i medesimi soggetti, che perseguano finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato il trattamento dei dati sensibili ***(Art.20)*.**

4.5 Principi applicabili al trattamento dei dati giudiziari

Come per il trattamento dei dati sensibili, anche i dati giudiziari possono essere trattati da soggetti pubblici (non economici) solo se ciò sia espressamente autorizzato da una norma di legge o da un provvedimento del Garante i quali specifichino le finalità di interesse pubblico, i tipi di dati trattati e le operazioni eseguibili. Se non interverranno tali atti il trattamento degli stessi dovrà essere sospeso perché costituirebbe un illecito, con conseguenti responsabilità di diverso ordine ***(Art.21)*.**

Le amministrazioni pubbliche hanno, quindi, l'obbligo di:

- rendere trasparenti ai cittadini quali informazioni sono raccolte
- chiarire come utilizzano queste informazioni per la finalità di rilevante interesse pubblico individuate con legge

Tali indicazioni devono essere trasfuse in un atto regolamentare cui va data ampia pubblicità. Non si tratta di un mero adempimento formale poiché da tali regolamenti discenderanno effetti sostanziali per i cittadini interessati. Alcuni schemi di regolamento sono stati di recente sottoposti al Garante, il quale si è espresso in senso positivo, in particolare per le amministrazioni provinciali e comunali. Infatti, considerata l'ampiezza del settore, il Codice ha previsto la possibilità che siano redatti schemi tipo per insiemi omogenei di amministrazioni, sui quali può essere pertanto espresso un unico parere.

5 ADEMPIMENTI

Di seguito sono elencati gli adempimenti previsti in caso di trattamento di dati personali

- individuazione delle figure previste dalla legge
- informativa all'interessato
- consenso
- autorizzazione al Garante per i dati sensibili
- notifica al Garante
- comunicazione al Garante
- misure di sicurezza

5.1 Individuazione delle figure previste dalla legge

Individuazione del Titolare
Quanto all'individuazione del titolare si possono verificare due ipotesi:
- impresa individuale: titolare del trattamento sarà il titolare dell'impresa
- impresa gestita in forma collettiva: titolare del trattamento sarà la società o l'ente nel suo complesso nella persona del legale rappresentante

Individuazione e nomina del Responsabile
- deve essere nominato per iscritto dal titolare che gli assegna precise istruzioni
- caratteristiche:
  - esperienza
  - capacità
  - affidabilità

Individuazione e nomina degli Incaricati
- devono essere nominati per scritto dal titolare o dal responsabile e compiere operazioni di trattamento
- operano su indicazioni fornite dal titolare o dal responsabile

Il titolare o il responsabile deve:

- redigere un apposito mansionario attraverso il quale verranno fornite all'operatore tutte le indicazioni necessarie affinché si proceda correttamente, nonché provvedere alla loro formazione
- effettuare analisi e descrizione dei trattamenti
- predisporre un adeguato sistema di archiviazione di tutti i documenti in entrata ed in uscita

Ciò permetterà di verificare in ogni momento la posizione dei diversi soggetti in relazione al trattamento dei loro dati (es: se hanno acconsentito o meno al trattamento dei loro dati sensibili, se è stata loro inviata l'informativa).

E' importante sottolineare che gli incaricati pur effettuando materialmente il trattamento dei dati rispondono in caso d controversia con l'interessato solo nel caso in cui il titolare abbia fornito opportune e adeguate istruzioni e adottato le necessarie misure di sicurezza.

5.2 Informativa all'interessato

L'Informativa obbliga chiunque tratti dati personali a informare in modo chiaro ed esaustivo gli interessati in merito ai motivi del trattamento (finalità e scopi), ai criteri di elaborazione dei dati (sia manuali che informatizzati) all'obbligo o meno a fornire le informazioni, alla durata dei trattamenti e a dove rivolgersi per esercitare i diritti di controllo sanciti dall'art.7 del Codice stesso ***(Art.13).***

In particolare:

- deve sempre essere fornita
- deve sempre essere preventiva al fine di ottenere un consenso informato
- deve contenere tutte le notizie che possono risultare utili all'interessato.

Eccezioni ai principi sopra esposti

- la possibilità di non indicare nell'Informativa gli elementi già noti all'interessato
- la possibilità di non indicare informazioni che potrebbero ostacolare funzioni ispettive e di controllo da parte di un soggetto pubblico
- la possibilità di posticipare l'informativa al momento della registrazione dei dati o della prima comunicazione di essi, quando i dati medesimi non sono ancora raccolti presso l'interessato.

Una informativa completa deve dunque contenere:

- finalità e modalità del trattamento
- natura obbligatoria o facoltativa del conferimento
- conseguenze del rifiuto a rispondere
- soggetti che possono conoscere i dati
- diritti dell'interessato
- titolare ed eventuale responsabile

L'informativa deve avere le seguenti caratteristiche:

- scritta o orale (la forma scritta è considerata prova certa in caso di controversia)
- chiara e intelligibile
- valida per tutte le operazioni del trattamento
- può valere per più titolari

5.3 Consenso

Il trattamento è ammesso con il consenso espresso dell'Interessato: (Consenso obbligatorio) ***(Art.23)***

- può riguardare l'intero trattamento o singole parti di esso
- è valido se espresso liberamente
- è valido se documentato per iscritto
- deve essere necessariamente manifestato per iscritto quando il trattamento riguarda dati sensibili.

Il consenso non è invece richiesto quando il trattamento: (Consenso facoltativo) ***(Art.24)***

- è necessario per adempiere ad un obbligo previsto dalla legge, regolamento, normativa comunitaria
- è necessario per eseguire obblighi derivanti da un contratto del quale l'interessato è parte
- riguarda dati provenienti da pubblici registri, elenchi, atti e documenti conoscibili da chiunque
- riguarda dati relativi allo svolgimento di attività economiche
- è necessario ai fini dello svolgimento delle investigazioni difensive ai sensi della l. n. 397/2000
- è necessario per eseguire un pubblico interesse del titolare nei casi indicati dal titolare

- è effettuato da associazioni, enti od organismi senza scopo di lucro
- è finalizzato unicamente a scopi di ricerca scientifica.

5.4 Autorizzazione al Garante per i dati sensibili

I dati sensibili possono essere trattati solo con il consenso espresso dell'interessato affiancato da una specifica autorizzazione del Garante su richiesta del titolare. Per tale richiesta vige il principio del silenzio-rigetto. Se il Garante non si pronuncia entro 45 gg della presentazione il titolare non può considerarsi autorizzato a trattare dati sensibili ***(Art.26).*** Il Garante ha appreso che ciò sarebbe stato troppo gravoso per l'intero attuale sistema. E' stato previsto a tale proposito un elenco di autorizzazioni generali per interi settori o per categorie di titolari. Le autorizzazioni generali rappresentano lo strumento più idoneo per assicurare:agli interessati uniformità ed effettività di garanzie al titolare, entro i limiti di cui si è detto, di prescindere dalla richiesta di autorizzazione

- N.1/2005: dati sensibili nei rapporti di lavoro
- N.2/2005: salute e vita sessuale
- N.3/2005: dati sensibili in associazioni e fondazioni
- N.4/2005: dati sensibili e liberi professionisti
- N.5/2005: dati sensibili in diversi ambiti
- N.6/2005: dati sensibili e investigazioni private
- N./2005: dati giudiziari

Efficacia delle suddette autorizzazioni: 30 giugno 2007

5.5 Notifica al Garante

Le disposizioni in materia di notificazione rappresentano una tra le più importanti innovazioni introdotte dal Codice. Infatti se in precedenza la notificazione era sempre dovuta salvo eccezioni, oggi invece, è dovuta solo nei casi espressamente previsti e, peraltro, secondo modalità più semplici.
Il titolare notifica al Garante il trattamento dei dati personali cui intende procedere, solo se il trattamento riguarda dati genetici, biometrici, di salute e vita sessuale per procreazione assistita, sulla personalità, sondaggi di opinione, rischio sulla solvibilità economica, situazione patrimoniale, corretto adempimento di obbligazioni, comportamenti illeciti e fraudolenti ***(Art.37)*****.**
La notificazione presentata al Garante è validamente effettuata solo mediante compilazione di un apposito modello predisposto dal Garante da compilare secondo le modalità impartite da quest'ultimo e da trasmettersi soltanto per via telematica o secondo altri sistemi che lo stesso Garante può individuare. Le conseguenze per l'omessa notificazione implicano l'applicazione di sanzioni amministrative e/o penali ***(Art.38)*****.**

5.6 Comunicazione al Garante

Il titolare del trattamento è tenuto a comunicare previamente al Garante le seguenti circostanze:

- Comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o da regolamento **(Art.39 Comma1)**
- Trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria **(Art.39 Comma2)**

Se il Garante non si pronuncia il titolare può ritenersi autorizzato a comunicare i dati, salvo diversa determinazione anche successiva del Garante (principio del silenzio-assenso)

5.7 Misure di sicurezza

Il Documento Programmatico sulla Sicurezza (DPS) definisce, ai sensi del decreto legislativo 30 giugno 2003, n. 196, (Allegato B) le misure di sicurezza per il trattamento dei dati personali presso le strutture organizzative dell'Ente e i criteri organizzativi per la loro attuazione.
La sua redazione e/o aggiornamento deve avvenire entro il 31 marzo di ogni anno.
Della sua redazione e/o aggiornamento deve essere riferito nella nota integrativa di bilancio

Contenuti:

- l'elenco del trattamento dei dati personali
- la distribuzione dei compiti e delle responsabilità nell'ambito dell'organizzazione preposta dei dati
- l'analisi de rischi fisici, logici e organizzativi che incombono sui dati
- le misure di sicurezza per garantire l'integrità e la disponibilità dei dati nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità
- criteri di ripristino dei dati cancellati e/o danneggiati
- piano degli interventi di formazione
- criteri per la sicurezza nei casi di incarichi attribuiti al di fuori dell'azienda
- criteri per la cifratura e/o isolamento di dati sensibili o giudiziari

6 RESPONSABILITÀ

6.1 Danni cagionati per effetto del trattamento

"*Chiunque cagiona danni ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile. E' incluso l'obbligo di risarcire la parte danneggiata anche del danno non patrimoniale"* ***(Art. 15).***
Il legislatore ha, in questo caso, equiparato l'attività di trattamento dei dati personali ad una attività pericolosa con ogni conseguenza in ordine all'onere della prova. Come sappiamo, per le attività pericolose vige il principio per cui il danneggiato può limitarsi a dimostrare il fatto storico da cui dipende, a suo dire, il danno; mentre spetta alla controparte dimostrare di aver adottato tutte le misure adeguate, richieste dal caso concreto, per evitare il danno stesso.

6.2 Profili di responsabilità

6.2.1 Titolare

E' titolare del trattamento il soggetto o l'ente che decide "in modo autonomo in ordine alle finalità e alle modalità del trattamento" sui contenuti delle informazioni, ivi compreso il profilo di sicurezza. Il titolare è il centro di imputazione degli obblighi e delle responsabilità.
Ha il compito di organizzare e vigilare sul processo di trattamento dei dati ed è il destinatario delle sanzioni previste per il mancato rispetto della legge.
Per questa ragione il titolare è una figura necessaria: non può esservi trattamento dei dati senza che vi sia un corrispondente titolare.
Quando le operazioni di trattamento dei dati vengono effettuate nell'ambito di una amministrazione pubblica, di una società o di un ente, il titolare del trattamento è la struttura nel suo complesso.
Non devono essere considerati come titolari le singole persone fisiche che rappresentano l'ente (esempio amministratore delegato, rappresentate legale, il presidente).
Tuttavia nel caso di strutture divisionali dell'Ente con aree di competenza separate, con effettiva autonomia, la singola divisione si potrà considerare titolare o co-titolare del trattamento.
L'ipotesi della co-titolarità (art.4 comma1) rappresenta un'evoluzione normativa che tiene conto dell'esperienza applicativa: si verifica quando più persone o più enti decidono di gestire in collaborazione tra loro, il medesimo trattamento dei dati, determinandone in comune le finalità, modalità e sicurezza.
Es: consorzio di imprese
Ogni co-titolare condividerà a titolo personale le prerogative e le responsabilità della normativa sulla protezione dei dati personali. E' importante rilevare infine che:

- la titolarità non è delegabile
- il titolare è colui che ha la visibilità esterna. E' infatti colui che interagisce in via preferenziale anche se non esclusiva, con il Garante e l'interessato

6.2.2 Responsabile

La figura del responsabile è, nell'organigramma previsto dalla normativa, il motore di operatività del sistema, rappresentando un istituto flessibile ed efficace per un miglior trattamento dei dati.
Il ruolo di responsabile può essere attribuito:

- alla persona fisica che all'interno dell'organizzazione aziendale ha le responsabilità di gestione delle attività che richiedono un trattamento sui dati (responsabile interno).
- ad un'entità terza che presta la propria attività al servizio del titolare, effettuando operazioni di trattamento sui dati, intervenendo direttamente nel processo produttivo del titolare (responsabile esterno)

6.2.3 Incaricati

Il titolare o il responsabile hanno il potere di incaricare per iscritto determinati soggetti, in relazione alla loro diretta operatività sui dati.
Detto incarico sembra avere per alcuni la natura di un mero conferimento di mansioni nonché di prescrizione di regole e di cautele.
La designazione degli incaricati è norma minima di sicurezza, oggetto del DPS.
Quando il trattamento è:

- **informatico**: è misura minima di sicurezza "l'aggiornamento periodico dell'individuazione dell'ambito di trattamento consentito ai singoli incaricati".
- **cartaceo:** sono misure minime di sicurezza "l'aggiornamento periodico dell'individuazione dell'ambito di trattamento consentito agli incaricati per lo svolgimento dei relativi compiti, la previsione di normali procedure per la conservazione di determinati archivi ad accesso selezionato e la disciplina delle modalità di accesso per identificare gli incaricati"

Gli incaricati, come è stato già detto, operano dentro la griglia di istruzioni loro impartite dal titolare e dal responsabile riguardante quali dati da trattare ed a quali fini, a quali banche dati accedere, quali misure minime di sicurezza e cautele comportamentali osservare.
In aggiunta, essi sono chiamati in causa dal codice per una serie di compiti meramente esecutivi ma di portata non trascurabile (estrarre dati dell'interessato e comunicarglieli anche oralmente, offrirgli visione mediante strumenti elettronici, trasporre i dati su supporto cartaceo o informatico oppure trasmetterli via internet ricevere l'informazione circa l'accertamento del Garante, se non c'è un responsabile designato o se lo stesso è assente).

Questa progressiva definizione dell'ambito esecutivo degli incaricati, unita alle esigenze di sicurezza fa da sfondo alla previsione del disciplinare tecnico secondo cui il DPS deve prevedere degli interventi formativi rivolti agli incaricati al trattamento dei dati (art.19.6).

Responsabilità civile
Risponde l'ente con tutto il suo patrimonio.
Rimane ferma, però, la disciplina dell'art. 2104 C.C. in tema di diligenza del prestatore di lavoro: se vi è violazione dell'obbligo di diligenza nell'adempimento delle istruzioni ricevute da parte del prestatore di lavoro (soggetto delegato) ciò darà luogo all'applicazione di misure disciplinari e dell'obbligo di risarcire i danni.

Responsabilità penale
Poiché la responsabilità penale è personale sarà compito del giudice ricostruire la dinamica del fatto e del suo autore.
Ipotesi di condotta attiva (trattamento illecito dei dati personali): il giudice dovrà indagare su chi ha realizzato la condotta.
Ipotesi di condotta omissiva (es: inosservanza dei provvedimenti del Garante) e qualora esista un responsabile, l'accertamento sulla responsabilità penale verterà sull'effettività della delega e quindi sulla concreta possibilità che il responsabile aveva nell'evitare la condotta criminosa.

7 PRIVACY E RAPPORTO DI LAVORO

Norme richiamate agli art. 113 e 114 del Codice:

- Art. 4 Statuto dei Lavoratori – Impianti audiovisivi
- Art. 8 Statuto dei lavoratori – Divieto di indagini sulle opinioni

"Resta fermo quanto disposto dall'art. 8 della L. n. 300/70" che pone il divieto di indagine a tutela del lavoratore ***(Art. 113)***
"Resta fermo quanto disposto dall'art. 4 della L. n. 300/70" che pone il divieto del controllo a distanza ***(Art. 114)***

7.1 Verifica del datore di lavoro sull'uso degli strumenti elettronici

Il datore ha il diritto di controllare il corretto uso degli strumenti di lavoro aziendali (art. 2086-2104 CC), nonché il diritto di essere risarcito per il danno economico derivante da un uso improprio di internet, del telefono aziendale ed ha altresì il diritto ad assumere provvedimenti disciplinari nelle forme previste dall'art. 7 dello Statuto dei lavoratori.

Esempio: uso del PC aziendale

Il rischio derivante da un possibile controllo del datore di lavoro sul PC aziendale utilizzato dal dipendente è quello di riunire i dati che consentono di ricostruire possibili movimenti, interessi abitudini ecc.
La domanda che ci poniamo è in che misura il dipendente può utilizzare il PC aziendale per fini personali.
Premesso che manca una normativa specifica su questo tema, in rispetto all'art.8 dello statuto dei lavoratori, si potrebbe ritenere che l'uso personale del PC è da ritenersi legittimo, per chi ne abbia l'utilizzo per ragioni di lavoro purché:

- l'uso personale avvenga al di fuori dell'orario di lavoro
- l'uso personale non impedisca o diminuisca la capacità del PC ai fini lavorativi o sia piratato

A questo punto ci chiediamo in che limite il datore di lavoro può accedere al PC utilizzato dal suo dipendente e rilevare così i suoi dati sia personali che lavorativi.
A questa questione potremmo dare risposta facendo riferimento agli art. 4 e 8 dello statuto dei lavoratori.
Ma in merito l'orientamento del Garante ed anche della più accreditata giurisprudenza è quello di ritenere che il diritto alla riservatezza dei dipendenti non può mutare il titolo di proprietà della strumentazione informatica che è dell'impresa***"(Art.113).***

Esempio: e-mail aziendale

L'interrogativo che si pone è se risulta possibile controllare la posta del dipendente in sua assenza.
Premesso che la corrispondenza è caratterizzata dalla segretezza e che alla stessa stregua va tutelata anche la posta elettronica, premesso anche che è fatto divieto di leggere i messaggi (reato penale), occorre fare un distinguo sulle e-mail aziendali.
La casella di posta elettronica è sì tutelata, ma quando a metterla a disposizione è il datore di lavoro perde tutta la sua riservatezza, in quanto strumento che l'azienda mette a disposizione del lavoratore al solo fine di consentirgli di svolgere la propria attività.
Quindi la mailbox aziendale, pur se personale, deve essere intesa come strumento di lavoro.
Personalità non significa necessariamente privatezza dal momento che la e-mail aziendale rimane un bene accessibile a tutti gli altri dipendenti autorizzati.

La problematica del controllo a distanza nell'attuale economia si pone a cavallo tra lecito e illecito ***(Art.114).***
Fatta salva l'antigiuridicità del comportamento intenzionalmente finalizzato alla sorveglianza del lavoratore "persona" è evidente che stiamo andando verso una società dove il "controllo" è divenuto elemento strutturale del vivere collettivo.

Tale divieto non deve intendersi in senso assoluto, ma occorre fare riferimento al fine discriminatorio, tenendo presente che si intende tutelare la libertà e la dignità del lavoratore. In rispetto al principio del bilanciamento di interessi tra le parti è prevista la concertazione con le organizzazioni sindacali.

Uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo

Uno dei principali temi posti in merito all'art. 4 dello statuto dei lavoratori riguarda la videosorverglianza.
La normativa, in merito, prevede il rispetto di alcuni principi quali:

- **Principio di liceità**
  Il trattamento di video sorveglianza è ammesso solo nei limiti e nel rispetto dei principi della legge

- **Principio di necessità**
  Necessario allo scopo perseguito, evitandone ogni uso superfluo e solo quando altre misure risultino insufficienti o inattuabili

- **Principio di proporzionalità**
  Il trattamento di video sorveglianza deve essere proporzionale allo scopo perseguito

- **Principio di finalità**
  Gli scopi perseguiti devono essere determinati, espliciti e legittimi

Premesso il rispetto dei principi sopra citati, secondo quanto dispone lo statuto dei lavoratori in merito alla eventuale installazione di impianti audiovisivi, occorre concordare con i rappresentanti dei lavoratori le relative modalità prima di procedere alla installazione.

Pertanto in questo caso si rivelano decisivi:

- una piena informazione ai dipendenti circa l'uso della video sorveglianza rilasciata secondo i dettami dell'art. 13
- la localizzazione esatta delle telecamere e delle modalità di ripresa, escludendo riprese intrusive della privacy dei lavoratori e privilegiando le riprese delle postazioni di lavoro
- la definizione e la regolamentazione del ruolo dei dipendenti o di terzi, (esempio guardie giurate) ammessi alla stazione di lettura
- le misure di sicurezza per evitare, la distruzione, la perdita o l'accesso non autorizzato alle riprese interne
- fornire le informazioni sul trattamento dei dati tramite sistemi di videosorveglianza ai dipendenti e a chiunque lavori nei luoghi in questione
- che sia trasparente l'identità del titolare del trattamento, le finalità della sorveglianza, nonché i casi in cui le registrazioni siano esaminate dall'amministrazione, il periodo di registrazione e quando la registrazione è trasmessa alle autorità giudiziarie

8 TUTELA E SANZIONI

8.1 Esercizio dei Diritti

I diritti sono esercitati con richiesta senza formalità al titolare o al responsabile ***(Art.8)*.**

- alla richiesta è fornito idoneo riscontro senza ritardo
- non può essere richiesta la rettificazione o l'integrazione di dati personali di tipo valutativo, relativo a giudizi, opinioni o apprezzamenti di tipo soggettivo
- modalità di esercizio (art. 9) riscontro all'interessato (art. 10)
- la richiesta può essere rivolta a mezzo lettera raccomandata, telefax, posta elettronica
- può essere rinnovata non prima di 90 gg.
- l'interessato può delegare per iscritto, persone fisiche, enti, associazioni, e organismi
- i diritti di soggetti deceduti possono essere fatti valere da chi ha un interesse proprio o agisce a tutela dell'interessato o per ragioni familiari
- se l'interessato è una persona giuridica la richiesta è avanzata dal soggetto persona fisica legale rappresentante per statuto
- il titolare deve adottare misure per agevolare l'accesso ai dati da parte dell'interessato e per semplificare le modalità di richiesta e ridurre i tempi per il riscontro
- i dati possono essere comunicati al richiedente anche oralmente ovvero offerti con strumenti elettronici
- se vi è richiesta i dati vengono stampati, su cartaceo, ovvero trasmessi per via telematica
- se a seguito dell'accesso, non risultino esistenti dati personali del richiedente, può essere chiesto un contributo spese non eccedente i costi effettivamente supportati

8.2 Tutela amministrativa (Art. 141 -151 T.U.)

La tutela amministrativa è rimessa al Garante e può assumere le seguenti forme

- reclamo
- segnalazione
- ricorso
- eventuali provvedimenti del Garante

8.2.1 Il reclamo

Chi intende sottoporre al Garante una violazione della normativa può fare un "reclamo circostanziato" che contiene:

- fatti e disposizioni che si assumono violate e le misure richieste
- elementi identificativi del titolare, del responsabile e dell'istante
- in allegato si porta la documentazione utile ai fini della valutazione e l'eventuale procura al soggetto, ente o associazione che rappresenta l'interessato

Se il reclamo non è manifestamente infondato, il Garante può adottare uno dei seguenti provvedimenti, anche prima della definizione del procedimento:

- invito al titolare ad effettuare spontaneamente il blocco del trattamento risultato illecito
- prescrizione al titolare delle misure necessarie a rendere il trattamento conforme alle disposizioni vigenti
- blocco o divieto totale o parziale del trattamento risultato illecito o non corretto anche per la mancata adozione delle misure di cui sopra, oppure quando per la natura dei dati, per le modalità del trattamento, o per gli effetti che esso può determinare vi è il rischio di pregiudizio rilevante per uno o più interessati

- divieto integrale o parziale del trattamento che si pone in contrasto con rilevanti interessi della collettività

8.2.2 La segnalazione

Si ha segnalazione quando non è possibile presentare un reclamo circostanziato, nel senso sopra delineato.
Lo scopo della segnalazione è quello di sollecitare un controllo.
I provvedimenti emanati in seguito ai controlli, o anche prima della conclusione degli stessi, sono i medesimi provvedimenti previsti in caso di reclamo.

8.2.3 Il ricorso

Il ricorso può essere proposto sia innanzi all' l'Autorità Giudiziaria sia innanzi al Garante. Si tratta tuttavia di una possibilità alternativa per cui *"electa una via non datus recursus ad alteram"*.

Il ricorso può essere proposto soltanto dopo che la stessa richiesta è stata sottoposta al titolare o al responsabile ed è trascorso inutilmente il termine di 15 giorni (che può essere esteso a 30) ovvero è stato opposto alla richiesta un diniego anche parziale.
Il predetto "interpello preventivo" può essere omesso soltanto nei casi in cui il decorso del termine esporrebbe taluno a pregiudizio imminente o irreparabile.

8.2.4 Provvedimenti del Garante successivi al ricorso

Può essere disposto in via provvisoria il blocco in tutto o in parte di taluno dei dati ovvero l'immediata sospensione di una o più operazioni di trattamento.
Al termine del procedimento, il Garante, se ritiene fondato il ricorso, ordina con decisione motivata la cessazione del comportamento illegittimo indicando le misure a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione.
Il ricorso si intende rigettato in caso di mancata pronuncia entro 60 gg. dalla presentazione.
E' ammesso ricorso al Tribunale contro il provvedimento espresso o il rigetto. L'opposizione non sospende l'esecuzione del provvedimento.

8.3 Tutela giurisdizionale *(ART: 145 e ss)*

La giurisdizione è attribuita all'Autorità Giudiziaria attraverso due forme:

- ricorso
- opposizione alla pronuncia del Garante

Il foro territorialmente competente è quello ove ha sede il titolare del trattamento.

8.3.1 Il ricorso

Strumento di tutela dei diritti dell'interessato di cui all'art.7. Il Codice prevede la possibilità di far valere, alternativamente, tali diritti sia innanzi all'Autorità Giudiziaria, sia innanzi al Garante

8.3.2 L'opposizione alla pronuncia del Garante

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

8.3.3 Provvedimenti cautelari

Se ricorrono gravi motivi, il giudice può sospendere il provvedimento impugnato, in deroga alla regola generale dell'esecutività dei provvedimenti in pendenza di opposizione.
Quando sussiste il pericolo imminente di un danno grave ed irreparabile, il giudice emana i provvedimenti necessari con decreto motivato.
La sentenza non è appellabile, mentre è ammesso ricorso per cassazione.

8.3.4 Sanzioni amministrative *(Art.152 e ss.)*

Tabella 1 - Sanzioni amm.ve art. 152 TU e ss.

	min	**max**
Omessa o inidonea informativa - Dati comuni La condotta punita è la violazione della disposizione che contiene l'informativa	3.000 euro	18.000 euro
Omessa o inidonea informativa - Dati sensibili Giudiziari La condotta punita è la violazione della disposizione che contiene l'informativa	5.000 euro	30.000 euro
Cessione dei dati in violazione della disciplina prevista art. 162 1 comma Questo illecito consiste nella cessione di dati in violazione di quanto previsto dell'art. 16 A) e B)	5.000 euro	30.000 euro
Comunicazione dei dati sanitari da parte dei soggetti non autorizzati art. 162 II comma L'illecito consiste nella violazione della disciplina della comunicazione dei dati. E' previsto che, i dati idonei a rivelare lo stato di salute possono essere resi noti all'Interessato o a soggetti ex art. 82 II comma da parte di esercenti le professioni sanitarie ed organismi sanitari solo per il tramite di un medico designato dall' interessato o dal titolare.	500 euro	3.000 euro
Omessa o incompleta notificazione al Garante Ex art 37 e 38	10.000 euro	60.000 euro
Omessa informazione o esibizione al Garante Si sanziona il comportamento di chi non adempia alla richiesta del Garante di fornire informazioni e di esibire documenti. Il potere di richiedere è conferito al Garante in virtù dei suoi poteri di accertamento e di controllo che gli competono e che esercita principalmente nell'ambito delle decisioni relative a un ricorso.	4.000 euro	24.000 euro

Inoltre la sanzione è prevista fino al triplo quando la sanzione risulti inefficace in ragione delle condizioni economiche del contravventore.
Inoltre è prevista la sanzione accessoria della pubblicazione, per intero o per estratto del provvedimento di condanna in uno o più giornali indicati nel provvedimento che la dispone.

8.3.5 Sanzioni penali (art. 167 T.U. e ss.)

Trattamento illecito di dati comuni
E' un reato che ricorre quando il soggetto procede al trattamento dei dati in violazione degli art:

- art.18 principi applicabili ai trattamenti effettuati da soggetti pubblici
- art.19 principi applicabili al trattamento effettuato da soggetti pubblici di dati diversi da quelli sensibili e giudiziari
- art.23 norme sul consenso nel trattamento da parte di soggetti privati
- art.123 comunicazioni elettroniche, dati relativi al traffico
- art.126 dati relativi all'ubicazione dell'utente dei servizi di comunicazione elettronica
- art.130 comunicazioni indesiderate

E' punito con

- la reclusione da 6 a 18 mesi, se il fatto reca danno
- la reclusione da 6 a 24 mesi, se il fatto consiste nella comunicazione o diffusione

In questi casi è previsto il dolo specifico costituito dal fine di trarre per sé o per altri profitto

Trattamento illecito di dati sensibili
Costituisce reato il trattamento dei dati in violazione degli articoli:

- art. 17 trattamento che presenta rischi specifici
- art. 20 trattamento dei dati sensibili da parte di soggetti pubblici
- art. 21 trattamento dei dati giudiziari da parte di soggetti pubblici
- art. 22 Diffusione da parte di soggetti pubblici di dati sanitari, dati di sensibili e giudiziari.
- art. 27 trattamento di dati sensibili da parte di soggetti privati
- art. 45 trasferimento di dati all'estero al di fuori dei casi consentiti dalla legge

E' punito con la reclusione da 1 a 3 anni. Anche in questi casi è previsto il dolo specifico, al fine di trarre per sé o per altri profitto o di recare ad altri un danno.

Falsità della notificazione, o in atti, documenti o dichiarazioni al Garante
La condotta punita consiste nel comportamento di chi nella notificazione o in comunicazioni, atti documenti o dichiarazioni, resi o esibiti in un procedimento dinnanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie/circostanze o produce atti/documenti falsi.

È punito con la reclusione da 6 mesi a 3 anni, salvo che il fatto non costituisca reato più grave.

Omissione dell'applicazione delle misure di sicurezza
L'omessa adozione delle misure di sicurezza è punita con l'arresto sino a 2 anni e con l'ammenda da 10.000 euro a 50.000 euro.
E' prevista una clausola speciale di estinzione del reato, che consiste nella regolarizzazione dell'adempimento omesso, seguendo le prescrizioni del Garante e nel pagamento della somma pari al quarto del massimo previsto per la contravvenzione.

Inosservanza dei provvedimenti del Garante:
E' prevista la pena di reclusione da 3 mesi a 2 anni per l'inosservanza dei provvedimenti del Garante in tema di:

- autorizzazioni al trattamento dei dati sensibili
- autorizzazione al trattamento dei dati genetici da chiunque effettuato
- inosservanza dei provvedimenti emessi a seguito di ricorso oppure del provvedimento provvisorio di blocco o di divieto di trattamento emesso a seguito dell'esame di un reclamo

Non è viceversa prevista alcuna sanzione penale per l'inosservanza degli altri provvedimenti emessi dal Garante in sede di reclamo o a seguito di segnalazione

Altre Fattispecie
La violazione del divieto d'indagini sulle opinioni dei lavoratori e di controllo a distanza dei lavoratori sono punite con le sanzioni previste dallo statuto dei lavoratori (artt. 113 e 114). Si tratta della pena dell'ammenda da 154 a 1549 euro o l'arresto da 15 gg. a 1 anno, pene cumulabili nei casi più gravi.

Pene accessorie
E' prevista che la condanna per i delitti sopra elencati comporti la pubblicazione della sentenza *(art. 172)*.

CONCLUSIONI

La protezione dei dati personali è un argomento di grande interesse per lo Stato, ancor più alla luce dei recenti avvenimenti nazionali e mondiali. La materia, oltre alla normativa sopra brevemente descritta, si è recentemente arricchita di altre disposizioni: alcune applicabili a specifici soggetti come la Pubblica Amministrazione, i centri di comunicazione via Web (per intendersi i cosiddetti Internet Center) ed altre applicabili a tutti coloro che hanno in atto sistemi particolari di controllo come ad esempio i sistemi di video sorveglianza. La materia è in rapida evoluzione e completamento e già si profilano all'orizzonte disposizioni molto precise sul trattamento della posta elettronica o per particolari settori o trattamenti di dati. E' importante a questo punto sottolineare che, contrariamente a quanto si potrebbe pensare, l'applicazione delle misure di sicurezza previste dalla legge non deve essere vista solo come un'ulteriore imposizione normativa ma come un elemento di riflessione e di tutela per ridurre i rischi della perdita dei dati e assicurare, di conseguenza, la continuità della conduzione aziendale.