UNIVERSITÀ DEGLI STUDI DI PADOVA
DIPARTIMENTO DI INGEGNERIA
DELL'INFORMAZIONE CORSO DI
LAUREA TRIENNALE IN INGEGNERIA
INFORMATICA

Studio di fattibilità per la realizzazione di un piano di Disaster Recovery (Padova)

1 settembre 2010

Ringrazio,
sinceramente i miei genitori per il sostegno
costante e indispensabile a tale risultato,
il prof. Federico Filira per la sua disponibilità,
l'ing. Alberto Cavalletto per l'aiuto offertomi
durante la realizzazione del progetto
e i miei amici più cari.

Indice

Capitolo 1

Premesse

1.1 Concetto Business Continuity e Disaster Recovery

Il sistema informativo aziendale rappresenta le fondamenta di ogni attività di business intraprese da quest'ultima. Al giorno d'oggi ogni sistema informativo non può fare a meno del supporto di un sistema informatico anche se proprio questa automatizzazione è spesso causa di svariati problemi. Ogni caduta di servizio ICT provoca all'azienda danni diretti ed indiretti la cui entità dipende dal tempo di ripristino del sistema e dalla possibile o meno ricostruzione dei data base. Altri aspetti da valutare sono integrità e la disponibilità dei dati e il livello relativo che l'azienda deve saper soddisfare. Alla luce dei possibili intoppi e dando il giusto peso alla "Legge di Murphy" (Se qualcosa può andar male, prima o poi andrà male) è bene che ogni sistema informativo sia tutelato da un Business Continuity Plan -BCP- : piano logistico finalizzato a documentare il modo in cui un'organizzazione può far tornare operative le sue funzioni critiche entro un predeterminato periodo di tempo dopo un disastro o un grave danno. Il BCP è considerato come un processo globale che identifica i pericoli potenziali che minacciano l'organizzazione, e fornisce una struttura che consente di aumentare la resistenza e la capacità di risposta in maniera da salvaguardare gli interessi degli stakeholders, le attività produttive, l'immagine, riducendo i rischi e le conseguenze sul piano gestionale, amministrativo, legale. Al centro del BCP ci sono quindi i processi di business e in particolare quelli critici per l'azienda la cui interruzione può portare a significative riduzioni dell'operatività complessiva. Il Bcp non si occupa quindi genericamente della disponibilità e della continuità operativa di tutti i singoli processi aziendali, né tanto meno dei diversi componenti dell'infrastruttura Ict, ma affronta il problema da un punto di vista

più complessivo; in quest'ottica, la continuità operativa di alcuni sistemi può essere trascurabile.
Ora però sorge un'ulteriore domanda: quali sono gli eventi dei quali si occupa la Business Continuity? La risposta a questa domanda non è molto semplice tuttavia non è detto che una risposta ci interessi realmente. Gli eventi possono essere i più disparati, eventi naturali catastrofici, attentati terroristici e blackout ecc. Ogni singolo imprevisto può causare una perdita di operatività e tale operatività richiede un intervento attivo per essere ripristinata. Come anticipavo prima quindi, l'attenzione è posta più su come rimediare alla perdita di operatività, che sulle singole cause scatenanti.
Il processo di gestione della continuità operativa comprende anche il cosiddetto *Disaster Recovery*.
Un piano di Disaster Recovery (DRP) è un insieme di tecnologie, accortezze e azioni ben studiate atte a dar garanzia sulla continuità e la sopravvivenza dei processi di business e dei servizi al loro supporto in caso di eventi disastrosi. Il piano di disaster recovery, come già detto, è parte di un sistema più grande costituito dalla *Business Continuity*. La buona e sicura esecuzione di queste attività prevede che siano affrontati preliminarmente alcuni aspetti legati alla definizione dei possibili scenari di disastro, all'individuazione dei processi critici e al possibile coinvolgimento delle figure interne di riferimento o esterne all'azienda da contattare per l'attuazione del piano. Un buon piano di disaster recovery prevede che i sistemi coinvolti vengano classificati in base al loro impatto nel servizio offerto secondo consolidate definizioni: [2]

- Vitali
  Le relative funzioni non possono essere eseguite senza essere sostituite da strumenti (mezzi) di caratteristiche identiche. Le applicazioni critiche non possono essere sostituite con metodi manuali. La tolleranza in caso di interruzione è molto bassa, di conseguenza il costo di una interruzione è molto alto.

- Critici
  Le relative funzioni possono essere svolte manualmente, ma solo per un breve periodo di tempo. Vi è una maggiore tolleranza all'interruzione rispetto a quella prevista per i sistemi critici, conseguentemente il costo di una interruzione è inferiore, anche perché queste funzioni possono essere riattivate entro un breve intervallo di tempo (generalmente entro cinque giorni).

- Delicati
  Queste funzioni possono essere svolte manualmente, a costi tollerabili,

per un lungo periodo di tempo. Benché queste funzioni possano essere eseguite manualmente, il loro svolgimento risulta comunque difficoltoso e richiede l'impiego di un numero di persone superiore a quello normalmente previsto in condizioni normali.

- Non-critici
  Le relative funzioni possono rimanere interrotte per un lungo periodo di tempo, con un modesto, o nullo, costo per l'azienda, e si richiede un limitato (o nullo) sforzo di ripartenza quando il sistema viene ripristinato.

Un aspetto importante da non sottovalutare è che la criticità delle varie applicazioni, software di sistema e dati può essere un aspetto variabile, per questo deve essere valutata in funzione del periodo dell'anno in cui il disastro può accadere.
Spesso l'esecuzione di una Business Impact Analysis di dettaglio è considerata un'opzione a cui si cerca di sopperire magari utilizzando informazioni apprese da terzi con lo scopo di arrivare a delle situazioni che possono sembrare sicure fino all'arrivo del primo problema. Di fronte ad un blocco del sistema, in assenza della definizione preventiva degli scenari di disastro, l'IT attende una dichiarazione di disastro che il management potrebbe non essere in grado di dare con certezza per mancanza di dati oggettivi atti a valutare l'evento - in termini di possibili impatti - e in relazione ai costi di migrazione - totali, parziali - da sostenere. Queste incertezze che, impediscono una rapida e chiara decisione in merito all'attivazione del piano di DR, portano ad inevitabili ritardi che potrebbero causare gravi perdite e ulteriore disguido, non certo di poco conto, si identifica nell'attivazione di procedure studiate in precedenza facenti parte del piano di DR senza l'effettiva necessità. È pertanto assolutamente necessario individuare e specificare a priori il livello e la tipologia di disastro che si desidera affrontare e di conseguenza le modalità per misurarlo ai fini di riconoscerlo in tempi accettabili.

Il piano di disaster recovery potrebbe anche essere compito di aziende esterne (ASP -Application Service Provider-) ed in questo caso la definizione dei SLA -Service Level Agreement) diviene una componente fondamentale. Senza uno SLA ben definito potrebbero accadere svariati inconvenienti come la mancanza di risorse adeguate, costi dei servizi necessari troppo onerosi oppure l'eventuale manutenzione della documentazione non demandabile.
Altro aspetto da valutare con attenzione è la divulgazione di informazioni durante la progettazione e realizzazione del piano di DR. Spesso si verifica una costruzioni a compartimenti stagni, differenti teams specializzati in relative tecnologie e/o ambienti particolari arrivano al proclamare la loro parte di

soluzione senza essersi mai confrontati con le altre squadre. È invece utile che ogni gruppo sia allineato su quanto già prodotto e quindi riutilizzabile evitando così spiacevoli e costose ridondanze, inutili rivisitazioni e nel contempo ottenendo una maggiore integrazione della documentazione.

1.2 Osservazioni

Da una prima panoramica è ormai chiaro che il ciclo di vita delle informazioni nell'azienda e negli enti non si limita al solo, se pur ormai prevalente, contesto teleinformatico. Esso si estende anche ad altri contesti come quello manuale, della fonia, del copying e così via. Ciascuno di questi contesti è caratterizzato dalla disponibilità di risorse specifiche di ciascun contesto legate a tecnologie specifiche: locali, scrivanie, telefoni ecc. Questa considerazione ci consente di affermare che, in caso di disastro, l'aver predisposto, realizzato e collaudato un efficace Piano di Disaster Recovery è condizione necessaria ma non sufficiente per garantire la continuità dei processi aziendali. In altri termini, l'esistenza di un PDR garantisce solamente la funzionalità del solo contesto teleinformatico. *Tutto quello che non fa parte del solo sistema informatico lo si può trovare nel quadro complessivo della Business Continuity, di cui il Disaster Recovery è solo un aspetto.*

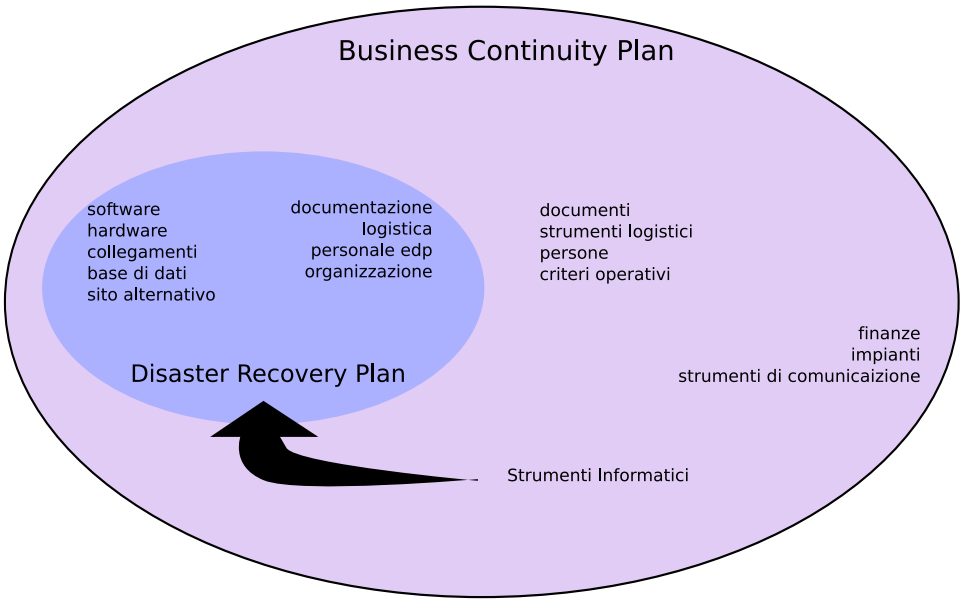


Figura 1.1: Piano di Business Continuity

Capitolo 2

Fasi di realizzazioni di un Piano di Disaster Recovery

Un PDR può essere suddiviso in sei macro fasi che delineano un susseguirsi di accorgimenti e azioni con relativo ordine temporale.[2]

- **Fase 0 - Definizione dei parametri di PDR**.
  In questa fase, partendo dallo studio dei processi aziendali e delle applicazioni software correlate, si perviene all'elencazione di queste ultime corredate dai rispettivi valori di criticità e dai tempi massimi che l'azienda può sopportare in relazione al fermo del servizio informatico.

- **Fase 1 - Definizione dei requisiti del Piano di Disaster Recovery**.
  Qui vengono forniti i criteri e le componenti strutturali del Piano i quali, una volta discussi ed approvati dalla direzione, consentono di procedere alle fasi realizzative successive. Da questa fase dovremmo quindi ottenere:

  1. modalità ed entità di utilizzo dei sistemi;
  2. configurazione hardware di minima per supportare il Piano;
  3. fonti di reperimento risorse hardware alternative;
  4. architetture di rete alternative;
  5. polizze assicurative;
  6. acquisizione e valutazione della documentazione necessaria;
  7. interfacce tra i vari sistemi di procedure;
  8. definizione della struttura organizzativa di gestione della crisi.

- **Fase 2 - Progettazione di dettaglio del Piano**.
  Definizione a livello dettagliato degli adempimenti procedurali, delle risorse software e hardware necessarie, dell'organizzazione della mobilità del personale, degli archivi e tutto ciò che può essere utile alla realizzazione del Piano.

- **Fase 3 - Implementazione del Piano**.
  Redazione degli adempimenti procedurali, acquisizione delle risorse software, hardware e logistiche e infine approntamento delle procedure di attivazione dell'hardware e dell'ambiente di esercizio.

- **Fase 4 - Test preoperativo**.
  Consiste nell'effettuazione del collaudo dell'intero Piano prima del rilascio in operativo e della relativa attività di formazione.

- **Fase 5 - Test operativi periodici e aggiornamento**.
  Effettuazione di esercitazioni periodiche di attivazione parziale e/o totale del Piano, nonché della definizione e messa in pratica dei criteri per la manutenzione ordinaria e straordinaria dello stesso.

2.1 Fase 0 - Definizione dei parametri di PDR

Il Piano di Disaster Recovery ha come obbiettivo il ripristino delle funzionalità del sistema informatico al verificarsi di evento disastroso, al fine di garantire la disponibilità, nei tempi predefiniti, delle risorse informatiche ritenute essenziali per i processi aziendali critici. Le risorse informatiche incluse nel Piano costituiscono i parametri e i criteri di Disaster Recovery. Obbiettivo della fase 0 è quello di individuare le applicazioni software critiche da inserire nel PDR.

2.1.1 Criteri per la definizione del dominio applicativo del PDR

Definiamo *Dominio applicativo* del Piano di Disaster Recovery l'insieme delle applicazioni software che devono essere ripristinate in caso di evento disastroso. Infatti, data l'entità degli oneri economici relativi alla realizzazione del PDR, si ritiene preferibile ripristinare solamente una parte delle applicazioni software, definite appunto critiche.

Per l'individuazione dei processi aziendali è utile considerare un alto livello di astrazione, tale livello è costituito dall'insieme dei macro-processi. Dopo

aver definito i macro-processi svolti dall'azienda, magari con l'aiuto di riunioni o interviste, è utile suddividere gli stessi in processi elementari ed in seguito occorrerà fare eseguire una classificazione dei processi in funzione della loro criticità così da determinare la relativa importanza per l'azienda. Grazie a questa procedura otteniamo una valutazione del contributo di ogni processo al raggiungimento del successo e il loro posizionamento rispetto alla missione aziendale. Una metodologia seguita per acquisire taluni risultati è detta "Metodologia Defender" che spiegheremo al momento dell'utilizzo.

2.1.2 Rivelazione di: applicazioni, hardware e reti.

Ora, come si evince dal titolo, si dovranno individuare e descrivere i componenti del sistema informatico dell'azienda, che dev'essere censito in tutti i suoi aspetti

2.1.3 Analisi e valutazione delle applicazioni

Segue ora un'analisi delle applicazioni appena censite che saranno ordinate per valori di criticità (Ca). Il valore di Ca è dato da

$$Ca = \sum_p (Vi \bullet Pa \bullet Vp)$$

cioè la sommatoria del prodotto dei valori Vi, Pa, Vp[*Vi: valore dell'impatto, Pa: peso dell'applicazione, Vp: peso del processo*] su tutti i processi coinvolti nell'applicazione. Ognuno di questi indicatori è calcolato sulla base di specifici criteri e scale che andremo ad analizzare a tempo debito.
Ovviamente il risultato ottenuto da questa procedura andrà poi valutato con l'aiuto di esperienza e buon senso dei componenti del gruppo di lavoro. Infatti potrebbe essere necessario includere o togliere applicazioni escluse o appartenute al nostro dominio per motivi di *tempo di ripristino*, *applicazione vincolante ai fini della missione* oppure per *legami di propedeuticità*.

2.2 Fase 1 - Definizione dei requisiti del Piano di Disaster Recovery

L'obbiettivo principale di questa fase sta nell'individuare le risorse necessarie alla realizzazione del PDR. Un aspetto da non sottovalutare è che non tutti gli utenti potrebbero essere meritevoli dei benefici del nostro PDR, spesso infatti alcuni fanno uso marginale dell'applicazione, svolgono quindi delle

attività che possono essere affrontate anche in seguito, quando l'operatività ordinaria stata ripristinata.

2.2.1 Centro Elaborazione Dati

Scelta critica di questa sezione è legata al CED (Centro Elaborazione Dati) perché punto di partenza per tutte le implicazioni organizzative e logistiche che andranno a caratterizzare il Piano stesso. Il Centro di Elaborazione Dati è un insieme coordinato di apparecchiature e servizi per la gestione dei dati ed è possibile implementare quest'ultimo in varie modalità a seconda delle aspettative da noi attese.
Una possibilità è data dal *CED ridondato*, cioè un Centro ricavato dalle già presenti risorse aziendali o con alcune integrazioni sufficienti a garantire il restore delle applicazioni presenti nel Piano. Questa metodologia garantisce un brevissimo tempo di risposta con conseguente disponibilità immediata del sistema ed altri vantaggi come l'assenza di degrado degli utenti e l'ambiente applicativo aggiornato on-line. Purtroppo questa soluzione seppur vantaggiosa dal punto di vista prestazionale impiega moltissime risorse finanziarie.
Altra soluzione, definita *Hot site aziendale*, consiste nell'avere un duplicato del "site business" originale completo di tutti le workstation necessarie con la possibilità di attingere ai dati utili per permettere il recovery del sistema. In condizioni di normalità potrebbe anche ospitare applicazioni di carattere marginale per l'azienda. L'Hot site garantisce un tempo di ripristino sull'ordine delle ore con un ambiente applicativo aggiornato all'ultimo backup. Anche in questo caso siamo di fronte a costi di esercizio altissimi e immobilizzazione finanziarie continue e consistenti.
Soluzione più economica consiste nell'appoggiarsi ad un *altro CED aziendale* che garantisce l'accesso in caso di disastro, questo ovviamente sarà determinato a priori con le relative verifiche e accertamenti del caso. I tempi di di ripristino saranno ovviamente un po' gonfiati rispetto alla soluzione precedente ma con costi nettamente inferiori.
Outsourcing, altra valida alternativa che garantisce una disponibilità del sistema in tempi adeguati con tempi di ripristino dell'ordine dei giorni. I costi del servizio potrebbero essere rimborsati da polizze assicurative adeguate e il tutto è garantito e preaccordato dal SLA (Service Level Agreement) accordato. I punti a sfavore di questa soluzione si possono trovare nelle continue revisioni del contratto, logistica precaria e sensibile degrado dell' operatività degli utenti.
Come ultima soluzione cito la *Empty shell aziendale*. In questo caso la struttura è simile a quella della tecnica Hot site, però sprovvista di sistemi di elaborazione. Qui otteniamo un costo irrisorio, dello spazio utilizzabile ad

altri scopi con tempi di ripristino sull'ordine di settimane. Gli svantaggi si possono individuare nell'ambiente tecnologico ed operativo da dover costruire da zero, collegamento in rete da predisporre e sensibile degrado dell'operatività degli utenti.

Alcune considerazioni.
La soluzione CED ridondato è una scelta estrema perché difficilmente giustificabile dal punto di vista economico a meno di esigenze estremamente stringenti. Analoga considerazione va fatta per la disponibilità di un Hot site aziendale infatti questa si presenta come la soluzione CED ridondante con la differenza di disponibilità di infrastrutture specifiche per le esigenze di Disaster Recovery. Diversamente dai due approcci appena analizzati, l'utilizzo di altro CED aziendale permette di ottenere buone prestazioni a costi relativamente contenuti. Naturalmente è possibile, anche in questo caso, richiedere tempi sull'ordine di ore, ma come ovvia conseguenza vi sarà un notevole aumento di costo. Soluzione che riscuote maggior successo tra le medie piccole imprese è l'utilizzo dell'Outsourcing. I centri servizi permetto la scelta tra vari livelli di soluzione che l'utente sceglie in base alle necessità, aspettative dei relativi clienti e soprattutto nel limite della disponibilità economica.

2.2.2 Definizione delle principali procedure

Una realtà da non sottovalutare è che il nostro PDR può essere studiato nei minimi dettagli però, è la componente umana a far la differenza tra un tempo di ripristino accettabile o meno. Si rende perciò necessario, prima dell'avvio di un Piano, definire alcune attività fondamentali:

- attuazione backup;
- predisposizione della logistica;
- predisposizione risorse umane.

Per quanto riguarda l'attuazione dei backup non credo siano necessarie molte parole, è sicuramente uno step fondamentale ai fini della riuscita del PDR e per questo è preferibile che i supporti destinati a tale servizio si trovino all'esterno del CED. La predisposizione della logistica ha l'obbiettivo di facilitare il ripristino delle applicazioni rendendo immediatamente disponibili le risorse necessarie e in questo senso semplifica l'avvio nei centri alternativi al centro disastrato.
In fine, la predisposizione delle risorse umane, vuole definire una struttura organizzativa che, in caso di evento straordinario, abbia ben chiaro i vari ruoli e relative mansioni da adottare.

2.3 Fase 2 - Progettazione di dettaglio del Piano

Per la progettazione di dettaglio del Piano dovranno essere redatti una serie di documenti che andranno a delineare l'evoluzione del nostro Plan Disaster Recovery. Ogni documento descrive una certa situazione del piano quindi esisterà una gerarchia temporale da tenere ben presente. In generale si possono presentare sei documenti:

- Predisposizione all'emergenza;
- Reazione all'emergenza;
- Notifica dell'emergenza;
- Trasferimento di dati e persone;
- Ripristino dell'ambiente lavorativo;
- Ritorno alla normalità.

Predisposizione all'emergenza.
Il primo documento dovrà chiarire la fase di backup, la logistica e la situazione delle risorse umane. Per il backup dei dati sarà necessario formalizzare tale procedura che garantirà la dovuta ridondanza presso il sito precedentemente definito. La predisposizione della logistica prevede documenti riguardanti tipologia e locazione del materiale, informazioni sulle postazioni di lavoro dei centri alternativi, elenco fornitori da contattare, scheda degli utenti autorizzati a lavorare nel CED alternativo con relative PDL e planimetrie del caso. Per quanto riguarda la sezione delle Risorse umane, troviamo documenti che delineano mansioni e dati del personale con una descrizione della struttura organizzativa per la gestione della crisi con i nominativi delle persone che prendono parte ai vari team.
Di seguito è riportato un organigramma di massima di una soluzione tipo:

Comitato di gestione della crisi: pianificazione e supervisione delle attività da svolgere in condizioni ordinarie e di crisi.
Coordinamento della riattivazione: gestione e coordinamento delle attività che si svolgeranno in condizioni ordinarie e di crisi.
Team di riattivazione: ripristino sistema informatico nel centro di backup.
Team di Help Desk: garantire le dovute sinergie e costante iterazione tra la struttura del CED ed i settori utenti inseriti nel Piano.
Team di rientro: gestione delle attività restanti nella sede dove è avvenuto il disastro e delle attività per la valutazione del danno e ripristino del CED

Figura 2.1: Organigramma soluzione tipo

ordinario.

Reazione all'emergenza.
In questo documento viene trattata la gestione delle situazioni di emergenza da parte del personale operativo. È molto importante differenziare le situazioni di crisi che possono verificarsi perché minime differenza possono dare luogo ad azioni completamente diverse tra loro. Basti pesare cosa comporta lo stesso danno in orari differenti, come potrebbe essere un orario di servizio anziché durante un periodo estivo. Il documento può svilupparsi in due macro sezioni: *Piano di escalation*, *Reperibilità del personale*.
La prima sezione è costituita da tutta una serie di azioni da compiere a seguito di eventi limitanti l'operatività del CED, solitamente nel formato di schede sintetiche per facilitare ed accelerare la comprensione. La seconda sezione definisce le procedure per l'allertamento del personale coinvolto nel piano di escalation con la relativa catalogazione dei dati di reperibilità di tutto il personale coinvolto.

Notifica dell'emergenza.
Questa documentazione affronta tutto ciò che riguarda la notifica dello stato dell'emergenza a partire dalla dichiarazione dello stato di crisi fino alla notifica a tutti i vari team. Anche in questo caso possiamo suddividere il problema trattato in :*Dichiarazione dello stato di crisi*, *Attivazione dei team operativi*, *Notifiche ai fornitori*, *Notifiche agli utenti*.

La dichiarazione dello stato di crisi è una delle fasi più critiche del piano di Disaster Recovery perché da essa scaturiscono tutte le azioni che coinvolgono l'azienda stessa e terze parti prendenti parte al Piano.
L'attivazione dei team operativi prevede solamente una sezione completa di tutti i dati di reperibilità riguardanti i partecipanti al PDR e una serie di norme per governare l'attivazione dei team.
Nella sezione Notifiche ai fornitori troviamo documenti predefiniti e già firmati per poter così permettere la notifica della crisi e di conseguenza la richiesta di erogazione dei servizi necessari. Qui è anche possibile inserire documenti di notifica per obblighi formali o di carattere amministrativo.
Le Notifiche agli utenti trovano spazio subito dopo aver dichiarato lo stato di crisi, perciò questa documentazione deve riportare comunicazioni di invito per l'utilizzo delle procedure d'emergenza previste dal Piano stesso.

Trasferimento di dati e persone.
Tutto ciò che riguarda problemi di logistica per l'attivazione del centro alternativo trovano spazio in questa sezione. Questa documentazione si rende necessaria solamente nel caso in cui il CED alternativo si trovi in altra sede rispetto a quella ordinaria e per questo motivo, cito solamente i vari documenti dovrebbero esser redatti.

- Trasferimento dati e documentazione al centro di backup:
    1. Procedura per il trasferimento dei dati e della documentazione
- Piano dei trasporti del personale:
    1. Tempi e modalità di trasporto
    2. Lista dei materiali da trasportare
- Organizzazione-ospitalità:
    1. Lista dei servizi
    2. Lista delle attrezzature disponibili presso il centro servizi

Restore dell'ambiente elaborativo.
In questa sezione troviamo la descrizione di tutte le procedure tecniche finalizzate al restore dell'ambiente.

- Restore del SI e ambienti di produzione;
- Restore dei collegamenti;
- Restore delle applicazioni;

- Restore dei dati;
- Procedure di backup del CED alternativo;
- Gestione degli elenchi delle password.

Ritorno alla normalità.
Una volta che la crisi è rientrata, è tempo di bilanci al fine di rendersi conto del danno economico subito, occorrerà quindi intraprendere le azioni legali necessarie con relative notifiche assicurative per poter così sperare di percepire il risarcimento adeguato. Come primo argomento perciò, troviamo *Rilevazione e valorizzazione dei danni*, segue *Notifica del danno all'assicurazione* ed in fine *Pianificazione del rientro*.
Per la rivelazione del danno va stilato un elenco degli impianti danneggiati con la relativa valutazione e sulla base di questo dovrà esser redatto un documento che affronti quali apparati andranno ristabilizzati, la consistenza degli investimenti da affrontare, tempi della disponibilità dei nuovi impianti e stima del rimborso.
Per la pianificazione del rientro sono previsti alcuni documenti che specificano le varie azioni, con l'adeguata sequenza temporale, da intraprendere con le relative indicazioni di tempi e modalità di rientro.

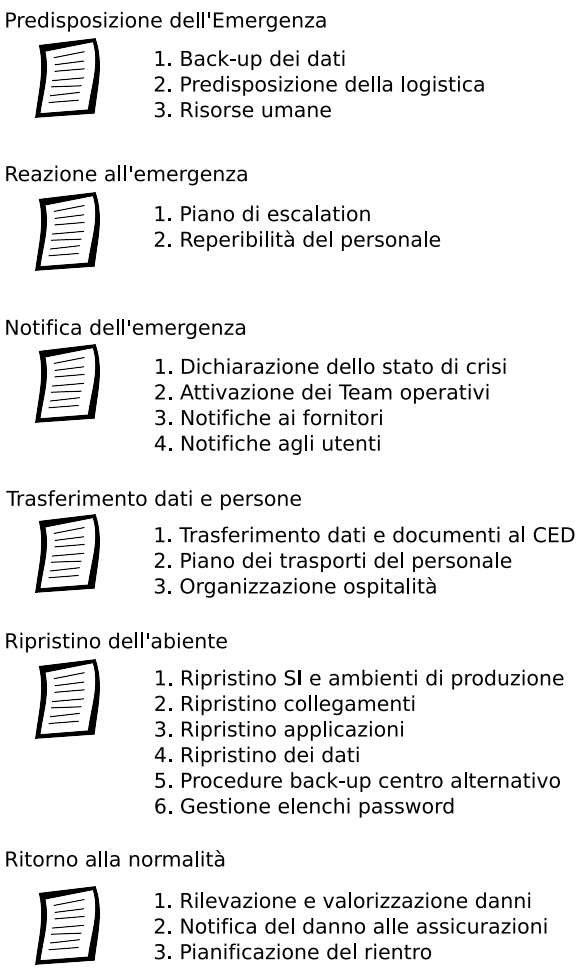


Figura 2.2: Documento di pianificazione rientro

2.4 Fase 3 - Implementazione del Piano

Questa fase si occupa principalmente della messa in opera del PDR, perciò andrà a rendere realtà ciò che è stato descritto nelle fasi precedenti. Quest' implementazione prevede tre attività principali:

- Redazione della documentazione prevista nel Piano;
- Pianificazione delle attività per la predisposizione dell'emergenza;
- Formazione del personale coinvolto.

Redazione della documentazione prevista dal PDR.
Qui, viene completata la documentazione relativa alle argomentazioni precedentemente affrontate, nello specifico vanno definite le modalità di realizzazione dei backup periodici con tutte le relative documentazioni anche dello stesso sito backup. Ora dev'essere anche affrontata l'implementazione dei vari team per la gestione della crisi ed è utile rendere facilmente reperibile, tramite distribuzione e/o esposizione, copia della documentazione redatta.

Pianificazione delle attività per la predisposizione dell'emergenza.
Arrivati a questo punto, dovrebbe essere terminata la fase di realizzazione del PDR, è quindi possibile suddividere le attività in due differenti tipologie:

- Attività in condizioni ordinarie;
- Attività da intraprendere come conseguenza dell'evento critico.

Nella prima suddivisione possiamo trovare tutta la documentazione relativa alle attività da intraprendere per ripristinare le attività vitali all'azienda nei tempi predefiniti.
La seconda categoria comprende le attività da intraprendere solamente in caso di crisi, perciò si andranno a pianificare e realizzare le attività per la predisposizione dell'emergenza ed è necessaria l'illustrazione di tempi e risorse di: effettuazione backup, stipula dei contratti, conferimento deleghe per attuazione Piano, stipula dei vari accordi con i dipendenti, acquisizione e predisposizione logistica, predisposizione e stanziamento budget annuale PDR. Il personale coinvolto dev'essere sensibilizzato circa l'importanza di un Piano di Disaster Recovery e non si ritiene sufficiente la messa a disposizione della documentazione redatta appositamente per affrontare la crisi, ma devono esser previsti dei corsi appositi di formazione specifica da rinnovarsi ad intervalli di tempo prestabiliti.

2.5 Fase 4 - Test preoperativo

Completata la "Fese 3" del nostro Piano, dovremmo avere uno strumento completo contro gli eventuali disastri.Il nostro prodotto però non è stato ancora testato e potendo essere in gioco l'azienda stessa è bene mettere alla prova il nostro lavoro. L'obbiettivo che ci prefiggiamo, dopo aver effettuato gli specifici test, è quello di ottenere un adeguato livello di fiducia circa la corretta progettazione e implementazione del Piano in modo da poter consentire la definitiva accettazione del Piano stesso.

2.5.1 Definizione criteri per accettazione del Piano

L'obbiettivo del test preoperativo è quello di valutare la conformità del Piano alle esigenze aziendali. Si procede con un esame quantitativo e qualitativo di alcuni parametri di conformità, che possono essere: *tempo di ripristino*, *efficienza del processo di riattivazione*, *costo attivazione e gestione PDR* ecc. Questi parametri appena citati sono solo alcuni dei possibili candidati alla valutazione, infatti questi possono essere presi in considerazione seguendo le esigenze e l'ambito aziendale. Tali parametri possono essere definiti in modo da:

- Includere tutti gli elementi fondamentali del PDR;
- Poter essere rappresentabili quantitativamente;
- Rendere la valutazione il più possibile oggettiva;
- Poter definire un range di accettabilità;

2.5.2 Effettuazione del test preoperativo

In questa fase è prevista la simulazione del intero Piano, cioè lo svolgimento di tutte le attività coinvolte con la convocazione di tutti i componenti dei team previsti con tutte le documentazioni del caso e valutazione dell'ipotetico danno. È molto importante non sottovalutare questa fase critica oppure affrontare i test in modo parziale per evitare spreco di risorse, sia umane che economiche, perché la buona riuscita di queste operazioni è un'ottima garanzia di efficacia.
Da questa simulazione noi vogliamo ottenere:

- Verifica dei parametri di conformità;
- Verifica imperfezioni di integrazione tra aspetti logistici, organizzativi e tecnici;
- Verifica della probabilità che insorgano imprevisti;
- Verifica della preparazione dei team.

Ovviamente la simulazione non deve portare al blocco delle attività ordinarie, anche se sarà inevitabile una riduzione dell'efficienza media.

2.5.3 Verifica di conformità del Piano

Il *Comitato di gestione della crisi* sulla base dei dati raccolti durante i test effettuati deve analizzare questi ultimi e decidere se:

- dichiarare la conformità del Piano e quindi **accettarlo**;
- promuovere un adeguamento, specificando ambito, modalità d'azione e comunicandolo al *Coordinamento alla riattivazione*;
- chiedere la ripetizione del test.

2.5.4 Adeguamento del Piano

L'adeguamento prevede che il test sia poi ripetuto con le stesse modalità del primo test, così otteniamo un riscontro se l'adeguamento è stato efficace. Le modifiche possono interessare: documenti, logistica, contratti, attività operative.

2.5.5 Accettazione del Piano

È compito del *Comitato di gestione della crisi* valutare i risultati emersi dai test e in base a questi dichiarare o non dichiarare la conformità del Piano e quindi si preoccuperà di notificare l'eventuale accettazione.

2.6 Fase 5 - Test operativi periodici e aggiornamento

2.6.1 Test operativi periodici

È necessario stabilire una periodicità, dove in tale scadenze vengano effettuati i test necessari alla verifica dell'efficienza del PDR, sia per un'evoluzione tecnologica inevitabile sia per mantenere il personale coinvolto pronto e consapevole delle proprie azioni. Solitamente queste periodicità non scendono sotto le due volte annue. Come si può intuire i criteri e le modalità dei test operativi periodici sono completamente analoghi al test preoperativo, si tratta solamente di ripetere questo per più volte per mantenere aggiornate le nostre certezze.

2.6.2 Manutenzione straordinaria

Durante il normale svolgimento dei test oppure durante una situazione ordinaria può succedere che si renda necessario una pronta verifica del PDR ed un eventuale adeguamento. In questi casi è necessario operare seguendo una specifica procedura di *manutenzione straordinaria* in cui devono essere definiti gli eventi critici che comportano una tale verifica e le operazioni da eseguire per rendere il PDR nuovamente conforme.
Vi sono molte aspetti che possono portare ad un adeguamento del Piano, alcuni li possiamo trovare in:

- modifiche nella composizione del team di gestione della crisi;
- modifiche nei dati di reperibilità;
- modifiche dei fornitori;
- modifiche dei contratti assicurativi.

Ogni modifica apportata, porta ad un'inevitabile revisione del Piano e come sappiamo, i cambiamenti in corso, anche se necessari, sono causa di maggiore complessità e il più delle volte è la chiarezza la vittima principale. Una gestione del PDR caratterizzata da frequenti modifiche può degradare pericolosamente anche l'affidabilità e l'efficienza, per questo, è necessaria un'analisi approfondita per accertare le effettive necessità di adeguare il Piano stesso: *Analisi della necessità di adeguare il Piano*. Tale analisi deve anche fornire quali sono le eventuali parti del Piano che devono essere riviste, la tipologia di modifica e l'autore materiale.
Si rende poi necessaria anche un'*Analisi della necessità di effettuare i test*, perché pur essendo il test elemento fondamentale per la verifica dell'affidabilità e funzionalità del PDR è un costo oneroso per l'azienda stessa. Pertanto, dopo un intervento di manutenzione straordinaria, bisogna valutare con estrema precisione la necessità o meno di affrontare il test del caso.

Capitolo 3

Aspetti legislativi

Dal 1996 in Italia vige il "diritto alla protezione dei dati personali" a cui comunemente ci si riferisce come "Legge sulla Privacy". Il 31 dicembre 1996 è entrata in vigore la legge n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali". Nel 2003 tale legge è stata abrogata e sostituita dal decreto legislativo 196/03 noto come "Codice in materia di protezione dei dati personali" entrato in vigore il primo gennaio 2004. Il primo articolo rende subito l'idea di cosa venga inteso per privacy nell'ordinamento italiano, infatti tale articolo recita: *Chiunque ha diritto alla protezione dei dati personali che lo riguardano.* Punto fondamentale è che la legge non tenta di impedire il trattamento dei dati personali ma di evitare che questo avvenga contro la volontà dell'avente diritto. Il Codice, in pratica, definisce la modalità di raccolta dei dati, gli obblighi di chi raccoglie, detiene o tratta dati personali e le responsabilità e sanzioni in caso di danni. Nel 1997 è stato costituito il "Garante per la protezione dei dati personali", un organo collegiale composto da quattro membri eletto dal Parlamento che ha il compito di vigilare sul rispetto delle norme sulla privacy.

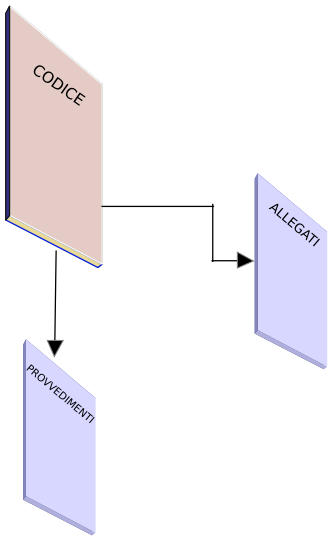


Figura 3.1: Quadro normativo

Il "Codice in materia di protezione dei dati personali" è il testo principale di riferimento per la privacy. Lo possiamo considerare come un testo unico che dal 2004 sostituisce, integra ed accorpa tutte le precedenti normative. Il codice contiene definizioni utilizzate ed i principi di riferimento. Le modalità pratiche per rispettare tali principi sono contenute negli allegati. Importanti sono anche i vari provvedimenti che il Garante ha emanato in questi anni. Questi tre documenti hanno valore di legge, quindi devono essere rispettati senza la concessione di alcuna eccezione. Periodicamente il Garante pubblica anche linee guida e modelli di riferimento per il rispetto degli adempimenti che sono però opzionali, sta quindi all'interessato decidere se prendere in considerazione questi aiuti.
Il codice ha tre sezioni principali :

1. disposizioni generali;
2. disposizioni relative a specifici settori;
3. norme relative alle forme di tutela, alle sanzioni ed all'ufficio del Garante per la protezione dei dati personali.

Di seguito una semplice figura per chiarire al meglio l'odine di importanza dei documenti citati.

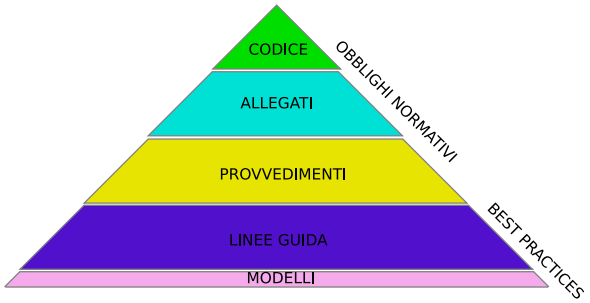


Figura 3.2: Gerarchia documenti

Ai fini di evitare ambiguità nell'interpretare il codice stesso l'articolo 4 recita alcune definizioni che è bene sapere; di seguito sono riportate quelle di nostro maggior interesse:[3, Art.4]

- **trattamento**, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

- **dato personale**, 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;

- **dati identificativi**, i dati personali che permettono l'identificazione diretta dell'interessato;

- **dati sensibili**, 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;

- **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;

- **responsabile**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- **interessato**, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- **comunicazione elettronica**, ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- **utente**, qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

Dell'articolo 4 appena citato è riportata solamente parte della terminologia utile alla piena comprensione della legislatura, sono stati scelti i termini più utili al contesto.

3.1 Articoli fondamentali

Per evitare un lavoro di copiatura, sono riportati solamente alcuni articoli di fondamentale importanza, altri saranno solamente citati.

Art 1. **Diritto alla protezione dei dati personali** : Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

Art 2. **Finalità** : Il presente testo unico, di seguito denominato codice, garantisce che il trattamento dei dati personali si svolga 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.

Art 7. **Diritto di accesso ai dati personali ed altri diritti** :
1. L'interessato ha diritto 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.
2. L'interessato ha diritto di ottenere l'indicazione :

- dell'origine dei dati personali;
- delle finalità' e modalità' del trattamento;
- della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
- dei soggetti o delle 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.

3. L'interessato ha diritto di ottenere:

- l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
- la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non e' necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

- per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché' pertinenti allo scopo della raccolta;
- 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.

Art. 11. **Modalità' del trattamento e requisiti dei dati** :
1. I dati personali oggetto di trattamento sono:

- trattati in modo lecito e secondo correttezza;

- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- 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.

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

Art. 13. **Informativa** :
1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa :

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le 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;
- i diritti di cui all'articolo 7;
- gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente 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.
3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.
4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.
5. La disposizione di cui al comma 4 non si applica quando:

- i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- 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;
- l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

Art. 15. **Danni cagionati per effetto del trattamento** :
1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.
2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Art. 16. **Cessazione del trattamento** :
1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:

- distrutti;
- ceduti ad altro titolare, purchè 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.

Art. 23. **Consenso**(1) :
1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.
2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.
3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.
4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

(1) La legge 27 febbraio 2009, n. 14, in sede di conversione con modificazioni del decreto-legge 30 dicembre 2008, n. 207, vi ha aggiunto il seguente comma:
Art. 44. **Disposizioni in materia di tutela della riservatezza** [...]
1-bis - I dati personali presenti nelle banche dati costituite sulla base di elenchi telefonici formati prima del 1° agosto 2005 sono lecitamente utilizzabili per fini promozionali sino al 31 dicembre 2009, anche in deroga agli articoli 13 e 23 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, dai soli titolari del trattamento che hanno provveduto a costituire dette banche dati prima del 1° agosto 2005. [...]

Art. 26 - **Garanzie per i dati sensibili** :
1. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti.
2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.
3. Il comma 1 non si applica al trattamento:

- dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che

con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

- dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria.

4. I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:

- quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

- quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

- quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a

rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

- quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111.

5. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

Art. 27. **Garanzie per i dati giudiziari** :
1. Il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

Art. 28. **Titolare del trattamento** :
1. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Art. 29. **Responsabile del trattamento** :
1. Il responsabile è designato dal titolare facoltativamente.
2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.
4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.
5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

Art. 30. **Incaricati del trattamento** :
1. 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.
2. La designazione è effettuata per iscritto e individua 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.

Art. 33. **Misure minime** :
1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34. **Trattamenti con strumenti elettronici** :
1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

- a) autenticazione informatica;
- b) adozione di procedure di gestione delle credenziali di autenticazione;
- c) utilizzazione di un sistema di autorizzazione;
- d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- g) tenuta di un aggiornato documento programmatico sulla sicurezza;
- h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

1-bis. Per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale, la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo di autocertificazione, resa dal titolare del trattamento ai sensi dell'articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte. In relazione a tali trattamenti, nonché a trattamenti comunque effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante, sentito il Ministro per la semplificazione normativa, individua con proprio provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico di cui all'Allegato B) in ordine all'adozione delle misure minime di cui al comma 1.

Art. 130. **Comunicazioni indesiderate** :
1. L'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato.
2. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo.
3. Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 23 e 24.
4. Fatto salvo quanto previsto nel comma 1, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.
5. É vietato in ogni caso l'invio di comunicazioni per le finalità di cui al comma 1 o, comunque, a scopo promozionale, effettuato camuffando o celando

l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'articolo 7.
6. In caso di reiterata violazione delle disposizioni di cui al presente articolo il Garante può, provvedendo ai sensi dell'articolo 143, comma 1, lettera b), altresì prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni.

Art. 167. **Trattamento illecito di dati** :
1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

Art. 169. **Misure di sicurezza** (1):
1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni.
2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

(1) Così modificato legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del decreto-legge n. 207 del 30 dicembre 2008

Art. 180. **Misure di sicurezza** :
1. Le misure minime di sicurezza di cui agli articoli da 33 a 35 e all'allegato B) che non erano previste dal decreto del Presidente della Repubblica 28 luglio 1999, n. 318, sono adottate entro il 31 marzo 2006.
2. Il titolare che alla data di entrata in vigore del presente codice dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle misure minime di cui all'articolo 34 e delle corrispondenti modalità tecniche di cui all'allegato B), descrive le medesime ragioni in un documento a data certa da conservare presso la propria struttura.
3. Nel caso di cui al comma 2, il titolare adotta ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti in modo da evitare, anche sulla base di idonee misure organizzative, logistiche o procedurali, un incremento dei rischi di cui all'articolo 31, adeguando i medesimi strumenti al più tardi entro il 30 giugno 2006.

Altre misure di sicurezza riportate nell'Allegato B.[4]

- Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

- I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

- Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

- Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Nota: Da tenere in considerazione il "Documento pragatico sulla sicurezza" art. 19 allegato B (appendice B) in caso di dati sensibili o giudiziari.

3.2 Sanzioni previste

Con l'articolo 44 del D.L. 30.12.2008 n. 207 sono state inasprite le sanzioni previste dal "Codice in materia di protezione dei dati personali", analizziamo comunque sia le sanzioni previste prima di questo decreto che il risultato delle modifiche apportate.

SANZIONI AMMINISTRATIVE	**AMMONTARE**
Omessa o inidonea informativa	Da € 3.000,00 a € 18.000,00
Omessa o inidonea informativa (dati sensibili, giudiziari, trattamenti che presentano rischi specifici)	Da € 5.000,00 a € 30.000,00
Cessione illecita di dati	Da € 5.000,00 a € 30.000,00
Violazione relativa ai dati personali idonei a rilevare lo stato di salute	Da € 500,00 a € 3.000,00
Omessa o incompleta notificazione	Da € 10.000,00 a € 60.000,00
Omessa informazione o esibizione al Garante dei documenti richiesti	Da € 4.000,00 a € 24.000,00

ILLECITI PENALI	**DETENZIONE**
Trattamento illecito dei dati	Reclusione da 6 a 24 mesi
Trattamento illecito dei dati (dati sensibili, giudiziari, trattamenti che presentano rischi specifici)	Reclusione da 1 a 3 anni
Falsità nelle dichiarazioni e notificazioni al Garante	Reclusione da 6 a 3 anni
Omessa adozione delle misure minime di sicurezza	Reclusione fino a 2 anni. Sanzione pecuniaria da € 10.000,00 a € 50.000,00
Violazione da parte dei datori di lavoro del divieto di effettuare indagini su opinioni politiche, controllo attraverso l'uso di impianti audiovisivi o altre apparecchiature art. 4 Legge n.300/1970	Arresto da 15 giorni ad 1 anno

Il DL 207/2008 ha apportato variazioni solamente ad alcuni illeciti:

SANZIONI AMMINISTRATIVE	**PRIMA**	**DOPO**
Omessa o inidonea informativa dell'interessato	Da € 3.000,00 a € 18.000,00	Da € 6.000,00 a € 36.000,00
Cessione illecita di dati	Da € 5.000,00 a € 30.000,00	Da € 10.000,00 a € 60.000,00
Violazione relativa ai dati personali idonei a rilevare lo stato di salute	Da € 500,00 a € 3.000,00	Da € 1.000,00 a € 6.000,00
Omessa o incompleta notificazione	Da € 10.000,00 a € 60.000,00	Da € 20.000,00 a € 120.000,00
Omessa informazione o esibizione al Garante dei documenti richiesti	Da € 4.000,00 a € 24.000,00	Da € 10.000,00 a € 60.000,00

Capitolo 4

Obbiettivi dello studio

Questo studio vuole, dopo un'attenta analisi di mercato guidata da prospettive, esigenze e necessità dell'azienda Telerete Nordest, valutare la miglior soluzione - in relazione della realtà presa in esame - che garantisca il ritorno alla piena funzionalità dei servizi prioritari nel minor tempo possibile, con la minima perdita di dati, nel rispetto delle norme vigenti e tutto questo pesato dall'aspetto economico.

Capitolo 5

Analisi delle esigenze

Telerete Nordest srl offre innumerevoli servizi tra cui possiamo trovare: PadovaWifi, UnipdWifi, MonseliceWifi, Videosorveglianza, Firma digitale, Servizi culturali e la disponibilità di molti altri prodotti. Il business di Telerete è perciò in gran parte vincolato all'erogazione continua di ciò che ne ha caratterizzato lo sviluppo e ne rimarca l'attuale posizione sul mercato, oltre alla vendita dei vari prodotti con relative consulenze e manutenzioni richieste dai clienti. La natura dell'azienda rende necessario, per una piena soddisfazione dell'utente finale, dei sistemi per aggirare e (nel peggiore dei casi) tamponare eventuali imprevisti più o meno gravi che possono intaccare ed interrompere le prestazioni offerte. Il Piano di Disaster Recovery andrà quindi implementato rispettando un tempo di ripristino dei "principali" servizi indicativamente inferiore alle quattro ore. In seguito verrà specificato ogni singolo servizio con il relativo tempo massimo di recovery.

Capitolo 6

Situazione di partenza

6.1 Contesto organizzativo

Telerete Nordest srl è dislocata in due sedi, una principale in Corso Stati Uniti 14/d (Padova) e la secondaria in Galleria Spagna (Padova). Il complesso principale trova dislocazione al quarto e quinto piano della struttura. Il quarto piano accoglie l'area amministrativa e commerciale, il quinto l'area tecnica e il callcenter. L'azienda dispone di due regioni datacenter dedicate poste in edifici differenti: Corso Stati Uniti, Galleria Spagna. Le due sedi sono collegate attraverso una rete in fibra per garantire una notevole velocità di trasferimento dati (oltre 10Mbit al secondo sia per l'up-stream sia per il down-stream).

6.2 Tecnologia utilizzata

L'azienda affida la gestione della propria informatizzazione ad un centinaio di server, opportunamente suddivisi in cluster, che si dividono tra fisici e virtuali. Essendo Telerete Nordest di esperienza decennale, coesistono tecnologie datate ed hardware molto più recente. Dislocate nelle varie sezioni -amministrativa, commerciale, tecnica, callcenter- troviamo un centinaio di workstation (desktop + pc), all'incirca una per ogni dipendente. Fa eccezione solamente la zona callcenter dove si alternano più persone sulle stesse postazioni, secondo i turni stabiliti.

Raid 1: Mirroring, copia esatte di tutti i dati.

Radi 5: Divisione dei dati a livello di blocco con ridondanza ottenuta attraverso bit di parità, distribuiti su tutti i dischi coinvolti nel raid.

Tutto il sistema attualmente utilizzato per il backup è gestito dal software **Bacula**, che garantisce il backup distribuito in rete, cioè la centralizzazione delle copie verso un unico server centrale. Il software è implementato secondo l'architettura client/server, con i client distribuiti sulle varie macchine a disposizione dell'azienda.

L'azienda può disporre di diciannove client distribuiti su macchine differenti ognuno destinato a veicolare verso il server Bacula principale, mole differenti di dati utili al ripristino dei vari servizi offerti.

6.3 Dati esistenti

6.3.1 Descrizione dei dati

Attualmente il sistema di backup prevede il recupero file di sistema e database presenti sui server aziendali, il sistema operativo e le applicazioni non vengono interessate da quest'operazione. Non sono presenti nei vari backup nemmeno i dati personali di ogni singolo dipendente.

6.3.2 Forme di archiviazione

Quasi la totalità dei supporti di archiviazione è costituita da nastri.

6.3.3 Meccanismi di aggiornamento

Il backup può essere gestito in maniera differente a seconda delle esigenze aziendali e/o di business. Vi sono cinque tipologie di backup:[14]

- Normale;
- Completo;
- Giornaliero;
- Incrementale;
- Differenziale.

Nel primo caso (normale), vengono copiati tutti i file selezionati e i file di backup vengono contrassegnati, cioè l'attributo di archivio = Off. In questo

caso per il ripristino di tutti i file è sufficiente avere a disposizione la copia più recente del nastro.
Il backup completo prevede la copia di tutti i file selezionati, però non ha alcun effetto sugli attributi di archivio. Può esser quindi utile tra una copia normale e incrementale: non avendo effetti sugli attributi sarà poi possibile riprendere con il backup incrementale.
Il backup giornaliero prevede la copia dei soli file interessati da modifica, oppure creati in giornata, senza però essere contrassegnati.
Backup incrementale e differenziale sono molto simili. Entrambi coinvolgono nella copia solamente i file modificati o creati dall'ultimo backup normale o incrementale, con l'unica differenza che la copia ottenuta dal differenziale non causa variazioni agli attributi di archivio, cosa che fa il backup incrementale.

Telerete Nordest prevede dei backup di giornata incrementali e backup completi settimanalmente e mensilmente.

6.4 Analisi di mercato

In questa sezione verranno trattate le possibili soluzioni che il mercato e la tecnologia attuale ci permette di adottare. La ricerca del più idoneo sistema che ci garantisca di attuare un efficace piano di disaster recovery può essere catalagota in due grandi insiemi:

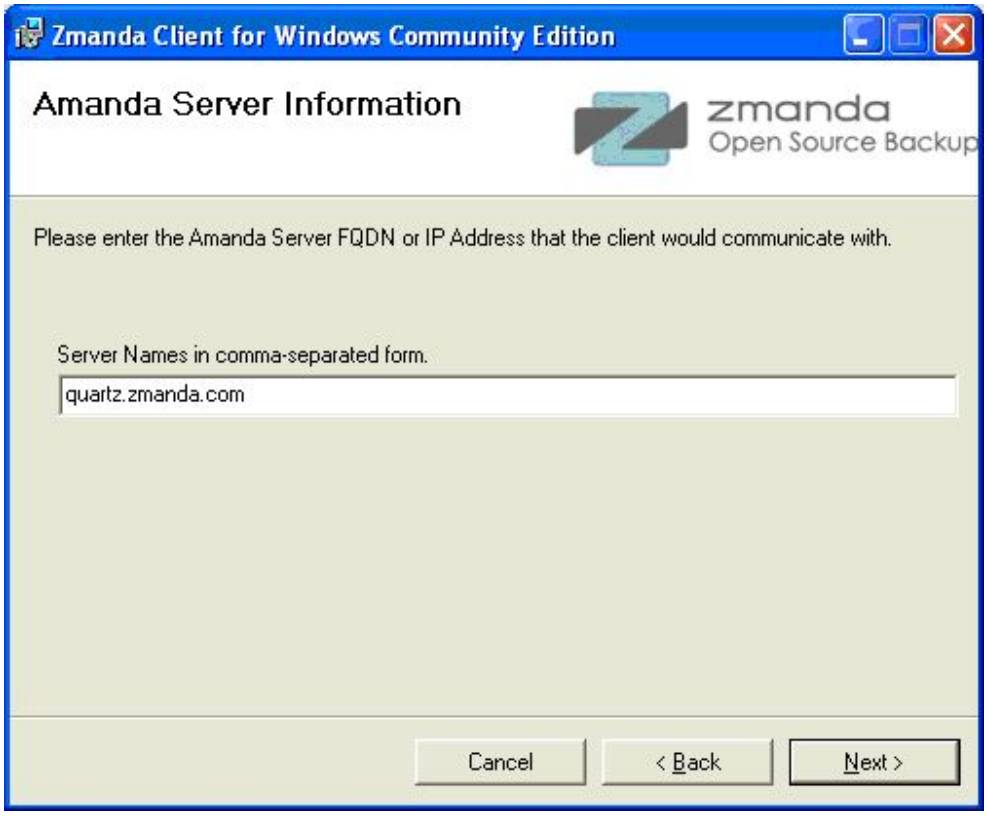
- Affidare la risoluzione ad un'azienda esterna. (es. symantec)
- Acquistare/scaricare software utili alle nostre finalità curando internamente l'installazione e l'aspetto formativo del personale coinvolto.

L'analisi verrà concentrata alle sole soluzioni di backup. Le soluzioni prese in considerazioni sono:

- Amanda;
- Cobian;
- IceMirror;
- Bacula;
- SyncBack;
- Lifekeeper;

- Symantec;
- Emc;
- I.Net.

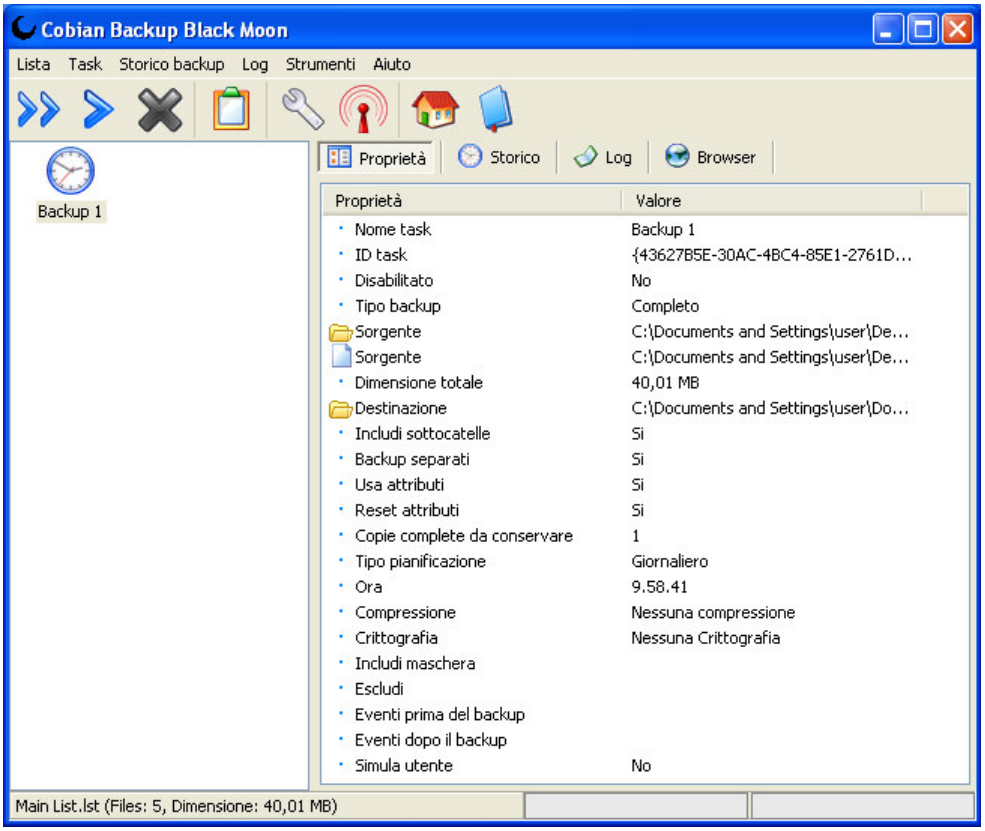
6.4.1 Amanda Open Source Backup



Descrizione:[5]
Amanda è un software open source per la centralizzazione dei Backup, permette cioè di collegarsi alle macchine presenti in lan ed archiviare i dati di nostro interesse su supporti dedicati. Amanda, l'Advanced Maryland Automatic Network Disk Archiver, è un sistema di backup che consente all'amministratore di configurare un unico server dedicato per eseguire il backup di più host sulla rete (su unità a nastro, hard disk o supporti ottici). Amanda utilizza dump native e/o strutture tar GNU e può eseguire il backup di un gran numero di stazioni di lavoro di più versioni di Unix. Questo software usa Samba, Cygwin o un client nativo di Windows per eseguire il backup di Microsoft Windows desktop e server.

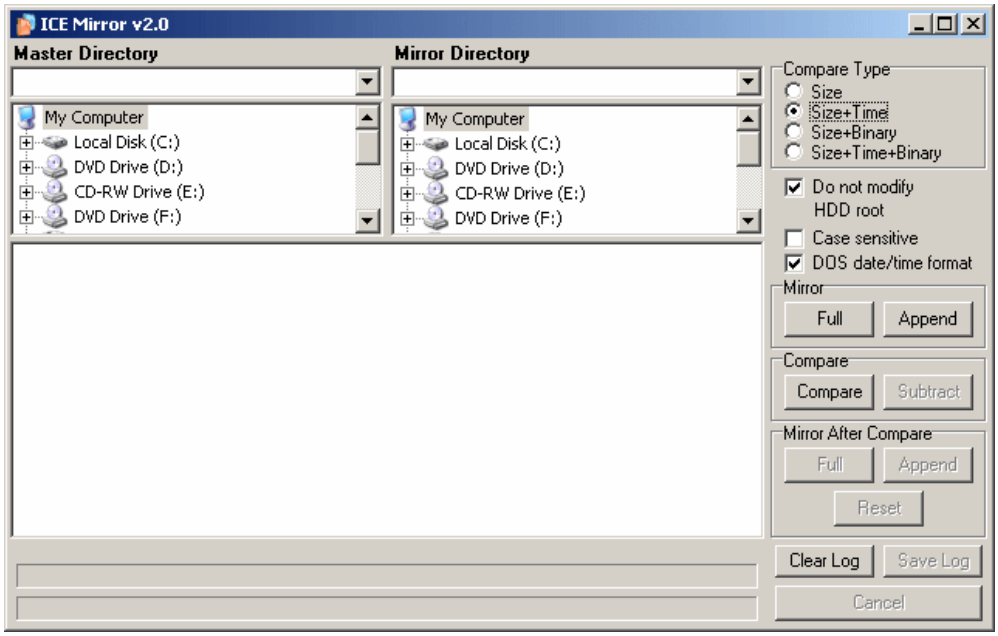
Costi:
Legati all'acquisizione: nulli.

6.4.2 Cobian Backup



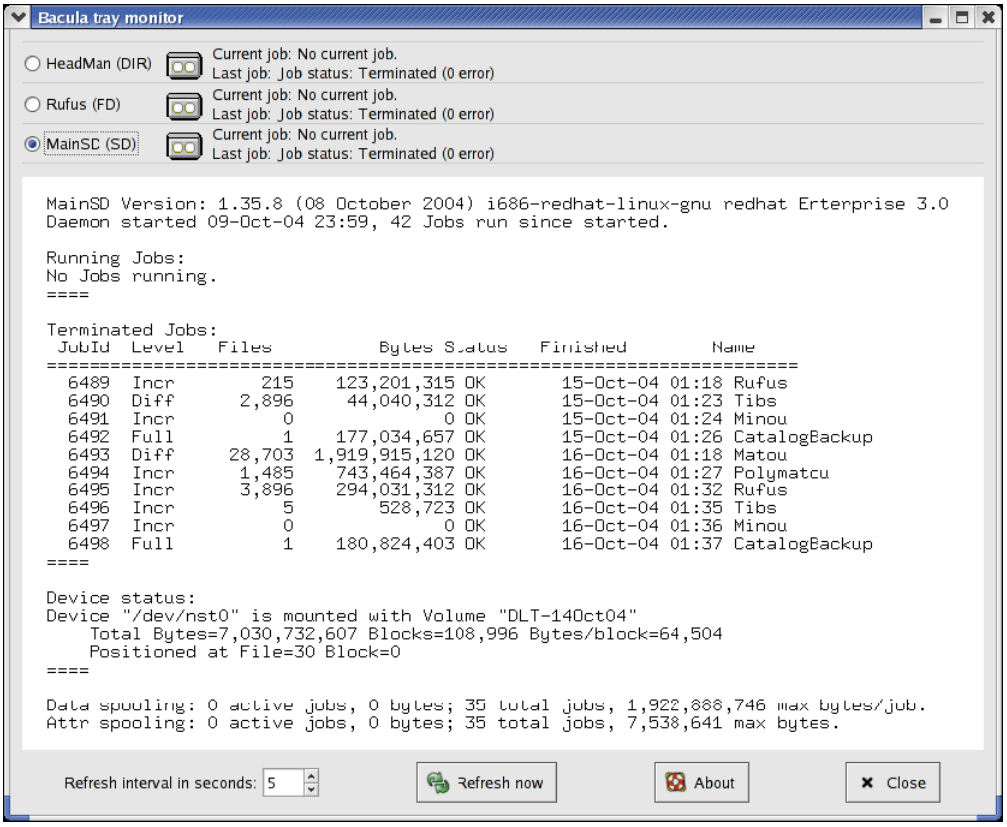
Descrizione:[6]
Il software Cobian Backup è un programma di utilità avanzato che può anche pianificare i tempi di backup e cosa andare ad archiviare sia sullo stesso computer che su altre macchine attraverso connessioni di rete e FTP. Cobian presenta due versioni, client e server, le quali rispettivamente lavorano sui vari host collegati alla rete e sul server dedicato al backup. È piuttosto un programma leggero che viene eseguito in background e mantiene si mantiene sincronizzato con il calendario di sistema. È in grado di archiviare periodicamente copia dei file in originale oppure in modalità compressa con numerosi tipi di formato sicuro e criptato.
Costi:
Legati all'acquisizione: nulli.

6.4.3 IceMirror



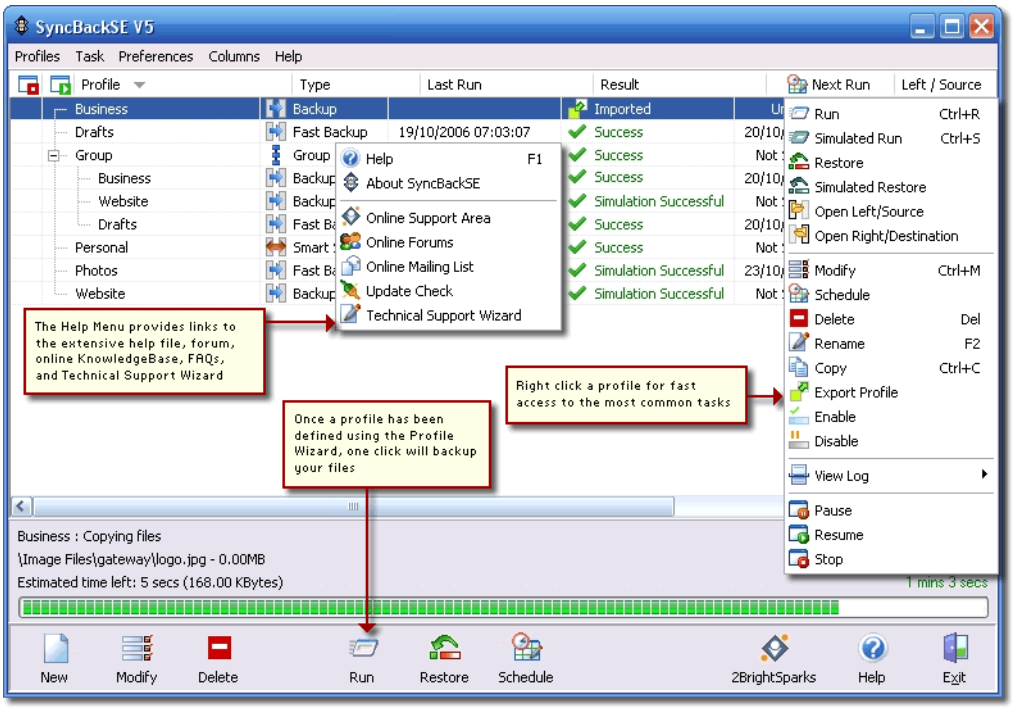
Descrizione:[7]
IceMirror crea o mantiene un duplicato esatto della directory originale. ICE Mirror confronta il mirroring in esecuzione con il mirroring alla directory principale e correggere eventuali disparità. ICE Mirror consente il mirroring incrementale e differenziale. Il primo permette di riportare sul supporto dedicato solamente i file che hanno subito una modifica dall'ultimo backup, il secondo invece, confronta i dati originali con l'ultimo backup consistente e riporta, su di un supporto differente da quello dove risiede il backup confrontato, i file nuovi e/o modificati.
Costi:
Legati all'acquisizione: nulli. (Licenza Freeware.)

6.4.4 Bacula



Descrizione:[8]
Bacula è un software openSource modulare che permette all'amministratore di sistema la gestione, il ripristino e la verifica dei dati di nostro interesse attraverso la rete grazie all'architettura client/server che lo caratterizza. Bacula attualmente supporta tre diversi database, MySQL, PostgreSQL e SQLite, una delle quali devono essere scelti per la costruzione di Bacula. Bacula possiede client per diversi sistemi operativi: Unix, Linux, Windows XP, 2000 e 2003. Bacula consente tre tipologie di backup: completo; differenziale e incrementale.
Costi:
Legati all'acquisizione: nulli. (Licenza Freeware.)

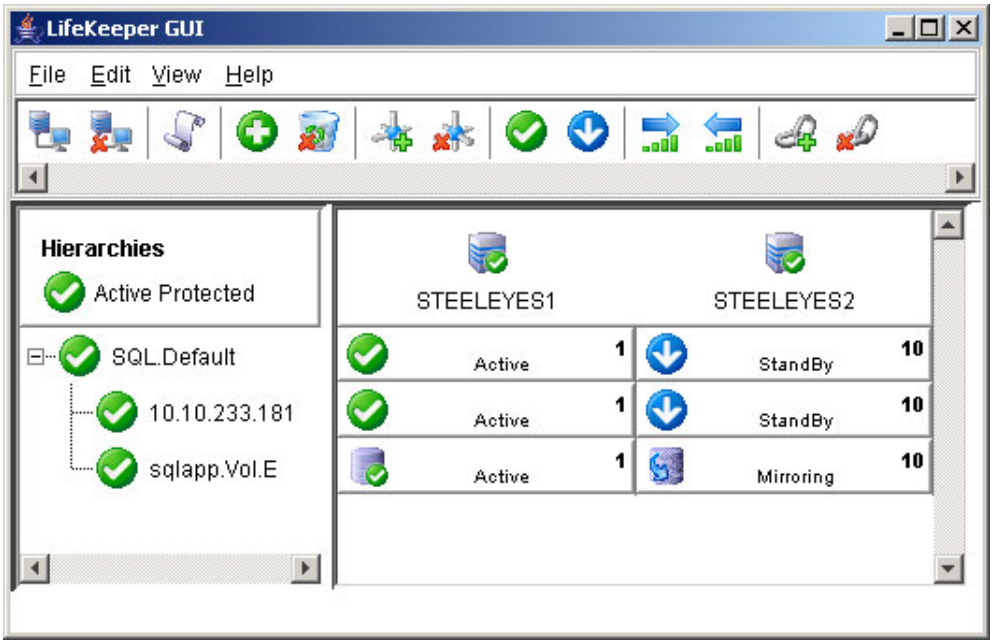
6.4.5 SyncBack



Descrizione:[9]
SyncBack permette di creare copie di sicurezza di file e cartelle facilitando anche la sincronizzazione tra sistemi differenti. Questo software mette a disposizione un'ampia possibilità di personalizzazione: è possibile indicare i file che debbono essere esclusi, come i vari documenti (vecchi e nuovi) devono essere trattati e molto altro ancora. SynBack è dotato anche di una funzionalità che permette la pianificazione delle operazioni di backup automatico, la compressione degli archivi di sicurezza in formato zip o, addirittura, l'upload degli stessi via FTP.
Costi:

- US$49,95 SyncBackPro;
- US$30,00 SyncBackSe.

6.4.6 Lifekeeper



Descrizione:[10]
È un prodotto di SteelEye Technology Inc, soluzione contro i fermi macchina grazie a clusterizzazione di macchine virtuali e processi, recovery kit per applicazioni critiche [SAP, Oracle, Exchange...] e Business Continuity. Lifekeeper monitora costantemente le macchine precedentemente stabilite e nel momento in cui un'applicazione sotto controllo non risponde, Lifekeeper trasferisce tutte le risorse di sistema e le richieste dei client al server di backup. Questa operazione, detta Failover, è trasparente agli utenti e quindi non impatta sulla loro operatività. Lifekeeper ha molti moduli interessanti che permettono svariate soluzioni alla maggior parte di imprevisti che puntualmente capitano. Per quanto riguarda la soluzione riguardante il Disaster Recovery se viene utilizzata su rete geografica o VPN permette di replicare i dati fra due o più server localizzati in sedi distanti fra di loro, ottenendo una soluzione di disaster recovery a basso costo. In caso ad esempio di blackout elettrico prolungato, o altro evento che renda inagibile la sede principale, è possibile far ripartire i servizi essenziali per l'azienda presso la sede di backup, avendo i dati aggiornati all'ultima transazione replicata.
Compatibilità:
Lifekeeper for Linux supporta sistemi basati su processori Intel e Intel compatibili. I sistemi operativi supportati sono Microsoft Windows, Linux RedHat e Linux Suse (Novel). Lifekeeper possiede inoltre un tool di amministrazione per la configurazione e il monitoraggio dello stato del cluster; il tool

può essere utilizzato o in modalità client/server, installando l'interfaccia su un sistema client, o in modalità web-based.

6.4.7 Symantec

Descrizione:[11]
Symantec è un'organizzazione leader globale nelle soluzioni di sicurezza, archiviazione dei dati e gestione dei sistemi. L'azienda ha l'obbiettivo di garantire la continuità operativa, rispettare i tempi di recupero con un'automazione delle più comuni operazioni di backup, clustering delle applicazioni e replica dei dati. Symantec offre molti prodotti e servizi che agevolano il raggiungimento degli obbiettivi prefissati da un piano di Disaster Recovery e Business Continuity, prevedendo anche dei corsi di formazioni per il personale interessato.
Costi:
I costi non sono disponibili a meno di un reale interesse verso il prodotto seguito da un'inevitabile iterazione con l'azienda stessa.

6.4.8 EMC

Descrizione:[12]
L'azienda garantisce che le soluzioni adottate permettano non solo di soddisfare gli attuali requisiti dei livelli di servizio relativi ai tempi di ripristino e alla perdita dei dati, ma anche riavviare rapidamente le applicazioni in seguito a un guasto ed eseguire la replica remota dei dati sfruttando tecnologie che riducono al minimo i costi di rete e la larghezza di banda. EMC aiuta le aziende a creare soluzioni personalizzate offrendo prodotti modulari che si impegnano a risolvere problemi come "protezione delle attività aziendali" , "backup", "protezione e replica remota continua dei dati" e molto altro.
Costi:

Anche in questo caso i costi non sono resi disponibili a meno di un forte interesse.

6.4.9 I.NET

Descrizione:[13]
L'azienda milanese fondata nel 1994 e fusa nel 2008 con BT Italia SpA è leader in Italia per soluzioni di Business Continuity e Disaster Recovery. I.Net prevede un approccio multi livello nell'abbracciare le necessità aziendali, consentendo di rispondere in tempi rapidi alle specifiche esigenze del business. Questa realtà offre, come gran parte delle alternative viste, software, hardware e accortezze al fine di garantire una continuità del servizio offerto dal cliente e (nel peggiore dei casi) una rapida ripartita del servizio rispettando i termini prefissati. Oltre a questi aspetti però, I.Net sembra curare in particolar modo l'approccio iniziale con il cliente, cioè in quella parte consulenziale mirata alla redazione dell'Analisi del Rischio e del BIA (Business Impact Analisys) necessarie per una soluzione che possa venir indossata più comodamente possibile.

6.4.10 Confronto soluzioni

SOLUZIONE	comp. UNIX	comp. MICROSOFT	COSTO	LICENZA
Amanda	✓	✓	/	GPL
Cobian		✓	/	Freeware
IceMirror		✓	/	Freeware
Bacula	✓	✓	/	GPL2/LGPL
SyncBack		✓	$30,00 - $49,95	Shareware
Lifekeeper	✓	✓	np	da acquistare
Symantec	✓	✓	np	da acquistare
EMC	✓	✓	np	da acquistare
I.Net	✓	✓	np	da acquistare

6.5 Vincoli

6.5.1 Normativi

I vincoli normativi richiesti, consistono nel rispettare le norme illustrate nei paragrafi precedenti.

6.5.2 Temporali

Tempo di recovery non superiore alle 24 ore.

6.5.3 Raccomandazioni

- Uso di software OpenSource;
- Soluzione che integri e utilizzi il software Bacula, per altro già a pieno regime sulle macchine dell'azienda.

Capitolo 7

Ipotesi di lavoro

7.1 Considerazioni

In base alle informazioni raccolte fin ora, si è certamente delineata una soluzione che dovrà (se possibile) essere pensata con l'utilizzo di prodotti OpenSource , rispettando così la filosofia dell'azienda, rendendo possibile eventuali modifiche e in ultimo, per non aggravare troppo il costo finale del progetto.
La struttura dell'azienda, ma soprattutto la dislocazione dei vari server rende necessario abbracciare una soluzione che permetta la gestione delle risorse di quest'ultimi attraverso la rete, con una centralizzazione finale dei dati. Grande considerazione merita anche la varietà di sistemi operativi che risiedono sulle macchine, possiamo trovare server Linux oppure Windows. La percentuale tra macchine Linux e Windows è circa del cinquanta per cento.
Il mercato offre innumerevoli soluzioni e la maggior parte di queste, particolarmente valide dal punto di vista puramente esecutivo. Entrano però in gioco molti fattori che riducono drasticamente le possibilità di scelta, come la necessità del OpenSource che esclude quindi tutte le soluzioni outsourcing. Gioca un ruolo fondamentale anche la conoscenza e l'esperienza che l'azienda ha ottenuto negli anni con l'utilizzo di Bacula, evitando così (se Bacula facesse parte della soluzione) eventuali corsi di aggiornamento o periodi di apprendimento di nuovo software.
La coesistenza di tecnologie differenti rende necessario l'utilizzo di una soluzione estremamente versatile, che possa nascondere all'esterno i vari problemi di compatibilità che inevitabilmente sorgeranno. Si rende necessaria quindi, la possibilità di far lavorare assieme hardware differenti, sistemi operativi differenti, con risorse differenti e database differenti (MySQL, PostgreSQL).
Nel corso delle varie interviste è emerso la causa principale che rende lento

ed oneroso il lavoro di ripristino di una macchina server. L'azienda dispone di server Linux e Windows ma, sono questi ultimi ad aggravare il tempo di recovery. Per poter ripristinare un server Windows, occorre caricare in primis il sistema operativo, reintegrare tutte le applicazioni necessarie alla dispensazione dei vari servizi, aggiornare il sistema con l'ultimo backup utile ed in fine adeguare il registro di sistema. Tutte queste operazioni richiedono all'incirca tra le sette e le otto ore.
Ulteriore problema si annida nella fase di backup. La virtualizzazione ha portato molti benefici ed agevolazioni, sia sul piano pratico (riduzione spazi e costi), sia nella fase di backup essendo la macchina virtuale rappresentata da una serie di file. Un normale salvataggio dei dati però, non è permesso a meno di un kill di tutte le virtualizzazioni coinvolte nell'operazione.

7.2 Ipotesi di soluzione

7.2.1 Amanda

Amanda è uno dei più popolari programmi open source per gestire situazioni di backup molto complesse. È un software dalle enormi possibilità, oltre che al creare backup incrementali, effettuarli su più volumi ha anche ottimi strumenti di compressione. Amanda si basa su architettura client-server quindi ciò comporterebbe l'installazione di tali applicazioni sul server principale e su ogni macchina indispensabile allerogazione del servizio offerto.
Durante lo studio del PD hanno acquistato priorità alcune specifiche di realizzazione:

- Efficiente metodo di restore della macchina danneggiata;
- Backup a caldo delle VM.

7.2.2 Bacula

Bacula è il software libero/Open Source leader come strumento di backup professionale e centralizzato. Sono disponibili client per Linux, Windows e Mac OSX, rendendolo una soluzione di rete multi-piattaforma.
Bacula è composto da diversi componenti e servizi usati per la gestione dei file di cui eseguire il backup e dove eseguirlo:

- **Bacula Director**: un servizio che controlla tutte le operazioni di backup, ripristino, verifica e di archiviazione;

- **Bacula Console**: un'applicazione che consente di comunicare con - Director;
- **Bacula File**: conosciuta anche come Bacula Client. Questa applicazione è installata nei computer di cui deve essere fatto il backup ed è responsabile dei dati richiesti dal Director;
- **Bacula Storage**: il programma che esegue l'archiviazione e il ripristino sul dispositivo fisico;
- **Bacula Catalog**: responsabile per mantenere l'indice dei file e il database di tutti i file, consentendo una facile localizzazione e ripristino. Catalog supporta tre diversi database: MySQL, PostgreSQL e SQLite;
- **Bacula Monitor**: consente di monitorare i demoni Director, File e Storage. Attualmente Monitor è disponibile solo come applicazione GTK+.

7.3 Analisi e soluzione da valutare

Una soluzione ideale che si presti ottimamente alla risoluzione del nostro problema dovrebbe essere di natura open source e permettere all'utente finale il minimo sforzo di apprensione nel minor tempo possibile così da arrivare ad un utilizzo a regime in poco tempo. I vari prodotti analizzati hanno portato allo stilare una tabella che riassume in poche righe gli aspetti principali presi in considerazione. Il range di votazione varia da un minimo di "1" (molto negativo) ad un massimo di "5"(molto positivo). Per quanto riguarda la voce "apprendimento", un voto basso, indica la necessità di uno sforzo considerevole al fine di ottenere una buona dimestichezza. Lo stesso vale per la voce "impatto", una votazione bassa sta ad indicare il forte impatto causato dal subentrare di questa soluzione con conseguenti inevitabili modifiche di processi aziendali.

SOLUZIONE	USABILITÀ	COMPRENSIONE	IMPATTO
Amanda	4	2	2
Cobian	3	3	2
IceMirror	3	2	2
Bacula	4	5	5
SyncBack	3	2	2
Lifekeeper	4	3	2
Symantec	5	3	1
EMC	4	3	1
I.Net	4	3	1

Alla luce di caratteristiche aziendali, esigenze, raccomandazioni, struttura interna e tenendo conto delle considerazioni appena emerse da un'analisi dei vincoli e dei prodotti presenti sul mercato otteniamo come soluzione più idonea a Telerete Nordest l'implementazione di un PDR portando avanti l'utilizzo di Bacula.

Capitolo 8

Progetto di massima

8.1 Obbiettivi

Gli obbiettivi principali possono essere raccolti in due sfere di competenza:

- Ridurre i tempi di recovery;
- Garantire una soluzione in linea con le attuali normative.

Il secondo obbiettivo comporta il rispetto delle norme minime di sicurezza sancite dal decreto legislativo 196/03 riportato in precedenza.

8.2 Funzioni del sistema

La soluzione studiata è caratterizzata dalle seguenti funzioni:

1. Garantire una rapida installazione del sitema operativo completo di tutte le applicazioni necessarie;
2. Permettere backup a caldo di server virtuali;
3. Gestire l'incompatibilità tra bacula e sistemi Microsoft (backup registro di sistema);

Funzione 1.
Per poter garantire una rapida installazione del sistema operativo, completo delle applicazioni presenti prima del crash, occorre creare un'immagine dell' intero disco. Per la creazione dell'immagine utilizziamo CloneZilla, valida alternativa opensource a programmi a pagamento come Acronis e Norton Ghost. Specifiche CloneZilla.

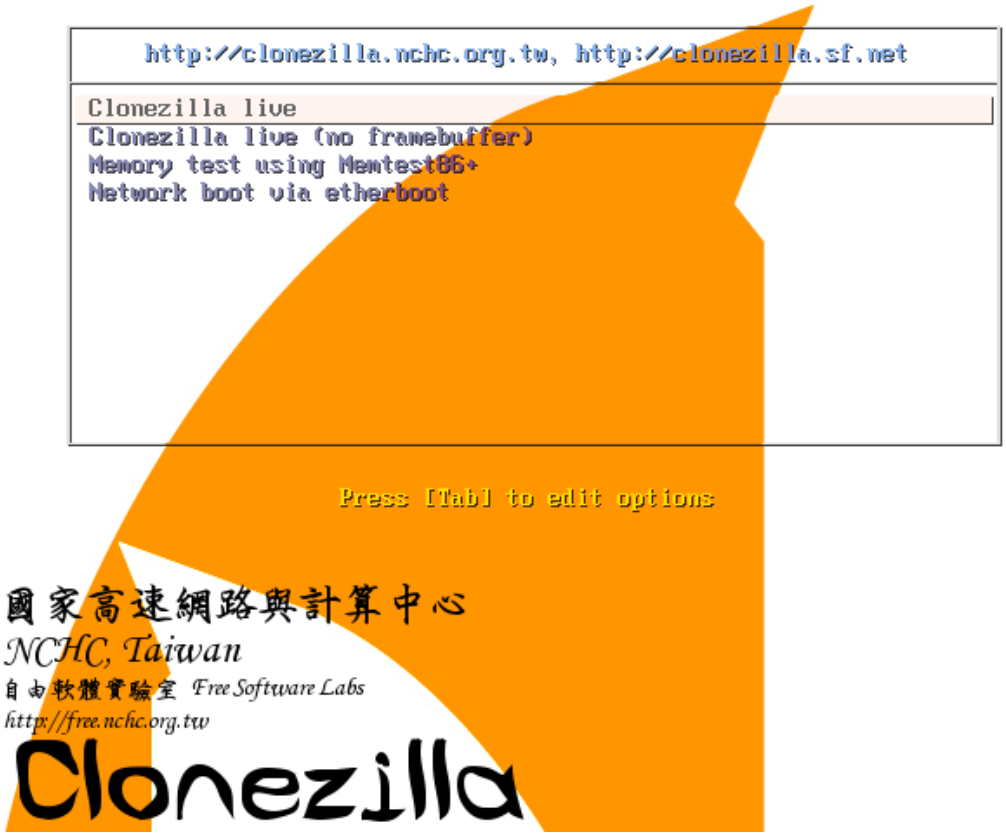


Figura 8.1: Screenshot Clonezilla

- Licenza GPL – Free Software.
- Filesystem supportati: ext2, ext3, ext4, reiserfs, xfs, jfs of GNU/Linux, FAT, NTFS of MS Windows, and HFS+ of Mac OS.
- LVM2 (LVM versione 1 non e' supportata) su sistemi GNU/Linux.
- Multicast nella versione Clonezilla SE (server edition), utile nel caso si debbano clonare o ripristinare diverse macchine in rete.
- Supporta Partimage, ntfsclone, partclone, e dd per clonare le partizioni. In oltre c'e' la possibilita' di clonare un intero disco suddiviso in piu' partizioni
- Utilizzando un ulteriore software, drbl-winroll sempre prodotto dai programmatori di Clonezilla,si ha la possibilita' di modificare l'hostname, group e SID del clone di una macchina Windows automaticamente.

Quest'operazione dev'essere però svolta solamente dopo aver creato un backup del registro di sistema il quale può essere fatto con un NtBackup. NtBackup è un'applicazione di backup inclusa in Windows Server 2003, se si dispone di Windows Server 2008 la cosa diventa un po' più complicata. In seguito verrà descritto come procedere.

Funzione 2.
Il realizzarsi di quest'operazione permette di ottenere file di backup senza dover interrompere i vari servizi che le rispettive macchine virtuali erogano ventiquattro ore su ventiquattro. VmWare stesso, con l'apposita suite VMware Consolidated Backup permette il backup di macchine virtuali senza interrompere gli utenti e le applicazioni. VCB richiede però un costo di licenza, quindi per questo delicato compito ci affideremo alla versione free di Trilead VM Explorer. La versione full è acquistabile per 490euro.

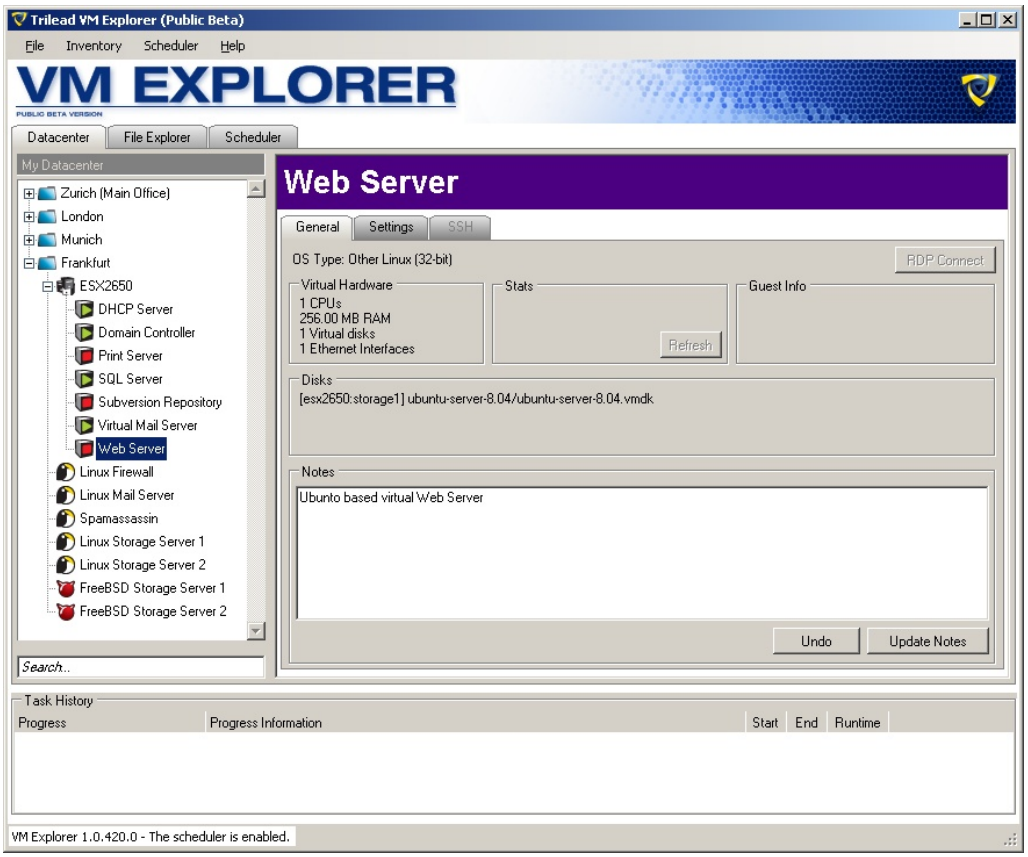


Figura 8.2: Screenshot VMExplorer

Nella seguente tabella riassuntiva possiamo trovare tutte le maggiori specifiche del sofware con le differenze tra la versione free e la pro.

SPECIFICHE	**FREE**	**PRO**
Backup&Restore for ESX virtual machines	SI	SI
Omessa o inidonea informativa (dati sensibili, giudiziari, trattamenti che presentano rischi specifici) Direct Copy: copy files with drag&drop between ESX/Windows/Linux/FreeBSD servers	SI	SI
Task Scheduler	NO	SI
SSH Client	SI	SI
Browse ESX, Linux and FreeBSD Servers	SI	SI
Backup from ESX 3.0.X/3.5 to ESX (SAN or local storage), Windows, Linux or FreeBSD	SI	SI
Backup from ESX 3i/4i to ESX (SAN or local storage), Linux or FreeBSD	NO	SI
Backup from ESX 3i/4i to VMX management station	SI	SI
Generate compressed backups	SI	SI
Migrate (clone) VMs from ESX 3.0.X/3.5 to ESX 3i/4i	NO	SI
Max Devices (ESX/Linux/FreeBSD host servers)	5	∞
Password protect	NO	SI
Daily Report via E-Mail	NO	SI
Commandline Interface	NO	SI
Start vSphere client with host credentials	NO	SI
Support	Email	Email
Price	Free	490€

Funzione 3.
Bacula non riesce a coinvolgere il registro di sistema di Windows nella propria routine di bakcup. Per ovviare a questo problema ci dovremmo servire di script appositi che prima di ogni salvataggio dati metta in opera NtBackup per ottenere un file che possa essere selezionato da Bacula.

8.3 Basi di dati

Il sistema informatico preso in considerazione coinvolge quattro tipi di database: Oracle, SQL server, mysql e Postgres. Anche in questo caso sarà necessario

implementare degli script che inneschino i relativi dump dei vari database così da poter coinvolgere anch'essi nel backup di Bacula. L'aggiornamento dei database avviene manualmente (per scelta dei dipendenti) oppure in automatico essendo la maggior parte delle applicazioni web-based.

8.4 Componenti tecnologiche

8.4.1 Componenti software applicativo

I software utili alla realizzazione del PDR sono:

- Bacula;
- CloneZilla;
- Trilead VM Explorer;
- NTBackup/Windows Server Backup.

8.4.2 Componenti hardware

La soluzione studiata non prevede l'integrazione o l'upgrade di componenti hardware, ma sfrutta ciò che è già a disposizione in azienda.

8.5 Linee guida del progetto

8.5.1 Aspetti critici

L'applicazione di software e motologie studiate affrontano vari passagi, talvolta critici, talvolta meno. È sempre bene chiarire e specificare a priori le possibili fonti di errore o intoppo per così meglio gestire gli eventuali imprevisti. La maggioranza delle criticità che potremmo incontrare sono da ricercarsi in:

- Restore dell'immagine su hardware differente (Clonezilla);
- Limitazione di VMExplorer(versione free);
- Disponibilità di spazio per backup macchine virtuali;
- Partizione di destinazione di dimensione maggiore-uguale alla partizione sorgente (Clonezilla);

Purtroppo non vi è alcuna soluzione foss che garantisca il restore di una partizione avviabile su hardware differente da quello presente durante la creazione dell'immagine stessa. Nel caso di rottura di qualche componente hardware è bene ripristinare la macchina sostituendo l'hardware corrotto con un componente del tutto simile, evitando così spiacevoli imprevisti. Se la riparazione avviene con hardware differente bisognerà provvedere manualmente all'installazione di driver appropriati.
Come visto nelle specifiche di VMExplorer, la versione free presenta una limitazione di cinque host per client.
Ultimo aspetto che se sottovalutato potrebbe portare a fastidiosi rallentamenti riguarda CloneZilla. La creazione di un'immagine della partizione d'origine (es.D), non è permessa se la partizione di destinazione (es. F) è minore di D. Quindi dev'essere sempre rispettata la relazione $D \leq F$.

8.6 Piano di realizzazione

8.6.1 Definizione delle fasi principali

Su richiesta di Telerete Nordest, non si è ritenuto necessario, causa organizzazione personale interno, lo sviluppo delle sei fasi sopra illustrate, che suddividono un Piano di Disaster Recovery. In questa sezione quindi, verranno illustrate solamente le varie fasi di realizzazione della soluzione informatica adottata con i relativi accorgimenti necessari.

Fase 1: Creazione immagine SO
Quest'operazione dev'essere intrapresa solamente a server perfettamente configurato e completo di tutte le applicazioni di nostro interesse.

- La prima operazione da fare è assicurarsi che nel menù di boot del bios della nostra macchina la scelta "CD-ROM Drive" sia la prima. Ora possiamo inserire il CloneZilla live CD (se si dispone della live di CloneZilla su USB flash drive basterà mettere come prima scelta " Removable Devices").
- quando ColoneZilla ci interroga sul da farsi proponendoci un menù, andiamo a selezionare la prima soluzione.

- scegliere la lingua.

- scegliere la tipologia di tastiera. La tastiera di default è quella degli Stati Uniti, l'opzione *Select keymap from full list* permette la scelta della tastiera a noi più consona.

- selezionare *Start Clonezilla* e premere *Invio*.

- selezionare la prima opzione: *device-immage*.

- nel menù " Mount Clonezilla immage directory", possiamo scegliere dove salvare la nostra immagine del disco.

- nel menù "Opensource Clone System" si dovrà scegliere su quale partizione salvare l'immagine che verrà creata.

- selezionate poi *Expert Mode*.

- ora utilizzate l'opzione *recovery-iso-zip*.

A questo punto la fatica è quasi finita. Ora di seguito si dovrà scegliere: l'immagine da ripristinare, il disco da recuperare quando il CD di ripristino o l'unità flash USB verrà utilizzata, la lingua in cui il CD di ripristino o un'unità flash USB verrà utilizzato, il layout di tastiera quando il CD di ripristino o l'unità flash USB verrà utilizzato, se creare file ISO (per CD / DVD) oppure file zip (per il flash drive USB) o entrambi.

Fase 2: Backup registro di sistema
Quest'operazione si rende necessaria visto l'impossibilità che Bacula ha di creare un backup che coinvolga anche il registro di sistema di Windows. Fino alla versione Windows Server 2003, si poteva contare sull'utility NTbackup, la quale consentiva con pochi passi di ottenere file bkf contenenti la copia del nostro registro. In Windows server 2008 NTBackup è stato sostituito dall'utility Windows Server Backup.
Nota: Mricosoft di default ha deciso di non accettare salvataggi dello SystemState sullo stesso disco ove risiede l'installazione di Windows, quindi se questo fosse necessario dovremmo forzare l'operazione come segue:

**

Eseguire regedit e aggiungere un nuovo valore DWORD (32 bit) chiamato "AllowSSBToAnyVolume" nel seguente percorso:
HKLM\SYSTEM\CurrentControlSet\Services\wbengine\
SystemStateBackup\AllowSSBToAnyVolume

Nei seguenti passaggi verrà illustrato come creare un backup schedulato dello stato dell'installazione di Windows sull'unità C (al bisogno prendere in considerazione la nota **), ovviamente se si desidera cambiare unità basterà

variare il percorso.

- creare un file batch, tipo “systemstate.bat” da posizionare in c:

- scrivere nel file batch, con un qualunque editor, la seguente riga di comando: *wbadmin start systemstatebackup -backupTarget:C: -quiet*

- ora scheduliamo un’operazione pianificata nei giorni e nei tempi che desideriamo per avviare il file batch appena creato.

Fase 3: Backup macchine virtuali
Come detto in precedenza, per il backup a caldo delle virtual machine presenti sui nostri sistemi, ci affidiamo a Trilead VM Explorer. Il software in questione è abbastanza semplice e intuitivo, ma in ogni caso propongo una breve guida all’utilizzo.

- Dal menù principale, selezionare il tab *Datacenter*

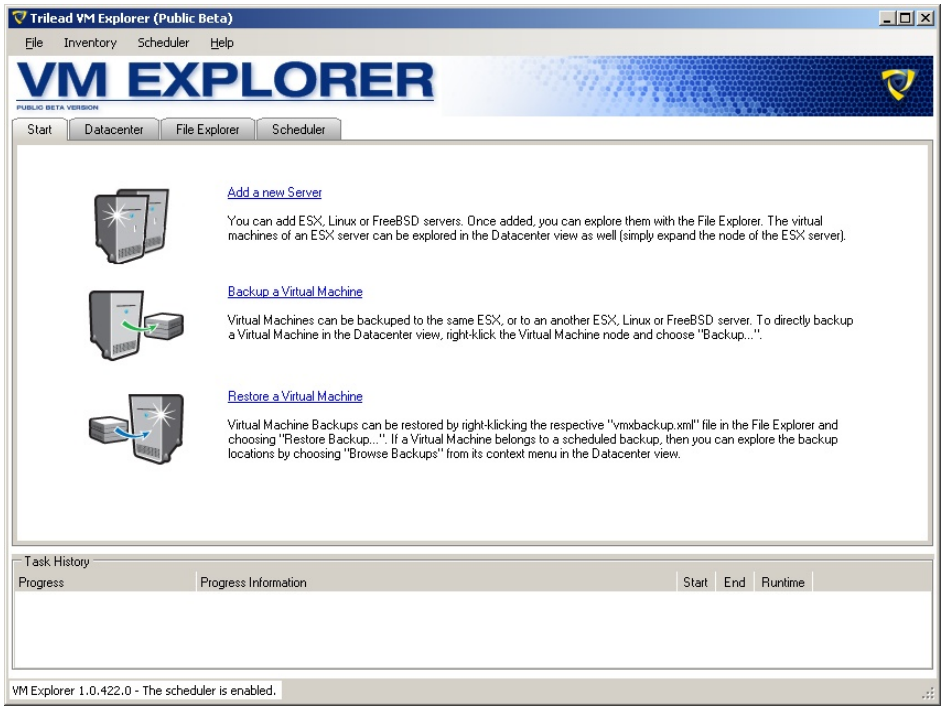


Figura 8.3: Screenshot VMExplorer

- ora espandere le VM del datacenter desiderato

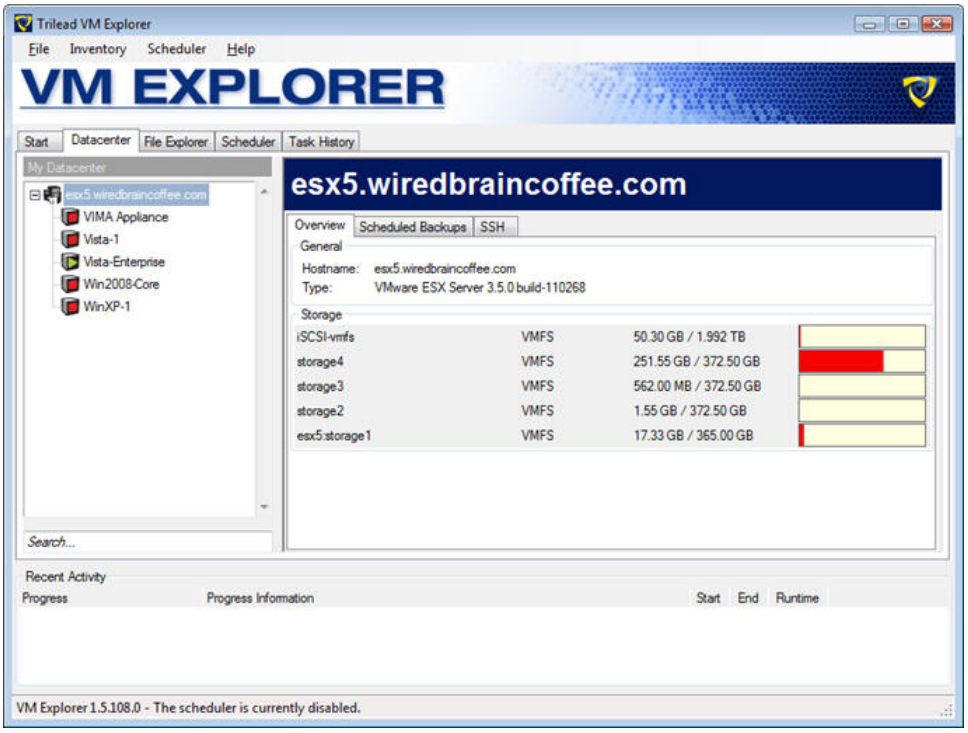


Figura 8.4: Screenshot VMExplorer (datacenter)

Nello screenshot si può notare che la scelta del datacenter è obbligata essendocene uno soltanto.

- selezioniamo *Backup* dal menù che ci appare clickando con il tasto destro sulla VM di nostro interesse

- ora se la configurazione del backup ci soddisfa, procediamo con un click sul pulsante *OK*.

Dopo queste semplici operazioni abbiamo ottenuto ciò che volevamo, un backup a caldo della macchina virtuale da noi specificata.

Il restore della VM è altrettanto semplice.
- Dal menù principale, se non è già selezionato, scegliamo il tab *Start*

- un click sull'opzione *Restore Virtual Maschine*

- apriamo ora la directory dove risiede il backup relativo alla VM che vogliamo ripristinare

- click con il tasto destro su *vmxbackup.xml* e dal menù scegliamo *Restore backup*

- non ci resta altro che confermare con un click su *OK* se il settaggio rispecchia la nostra volontà.

Fase 4: Backup dati
Il backup dei dati è già un'operazione di routine quotidiana svolta sui server di Telerete Nordest attraverso Bacula, quindi ulteriori precisazioni sembrano superflue. L'unica precisazione vuole ricordare che il backup ora dovrà coinvolgere anche i file .xml creati da VM Explorer e la cartella relativa al salvataggio del registro di sistema.

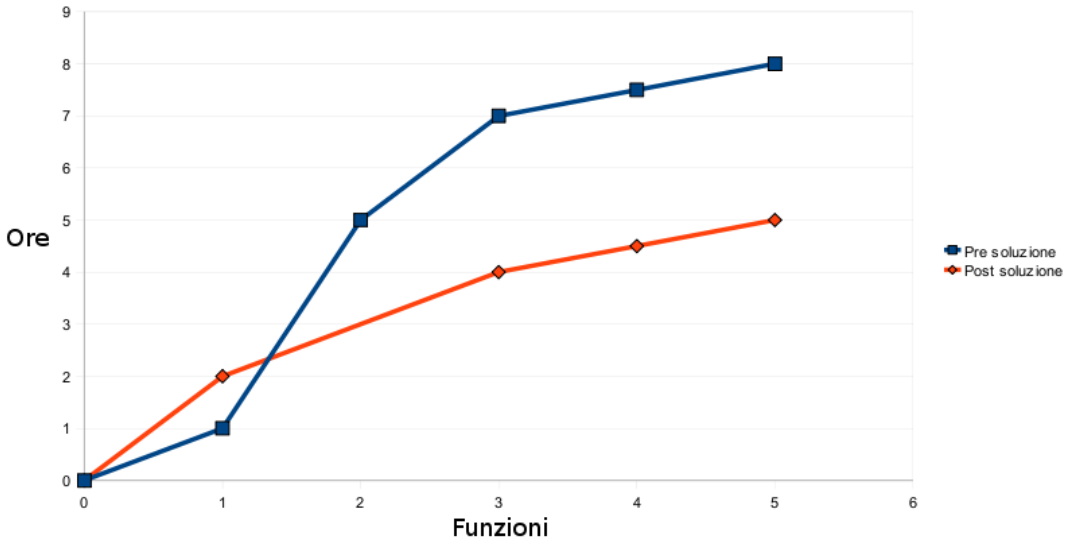
8.7 Analisi e valutazioni

Nel proporre tale soluzione si è cercato di rispettare la filosofia aziendale utilizzando solamente software open source. Per questo motivo non sono previsti costi aggiuntivi legati a licenze di prodotti oppure a servizi offerti da terzi.

È stato stimato (non verificato), che il tempo di recupero medio per il restore di un server equipaggiato con sistema operativo Microsoft si aggira tra le sei e le otto ore. Le cause principali che portano al dedicare un'intera giornata lavorativa ad un server danneggiato si rispecchiano in:

- caricare ex novo l'intero sistema operativo;
- installare tutte le applicazioni necessarie per permettere l'adempimento dei servizi forniti in precedenza;
- rendere nuovamente disponibili i dati caricando con Bacula l'ultimo backup concreto;
- aggiornare il sistema con il backup del systemstate;
- ristabilire tutti i servizi (considerate tali anche le macchine virtuali).

Con il PDR a pieno regime la seconda causa viene a sparire accorpandosi con la prima, ottenendo così in un'unica operazione il sistema forte di tutte le utility essenziali. L'aggiornamento del registro di sistema e il ristabilire i servizi sono, in relazione al tempo di ripristino, relativamente trascurabili rispetto agli altri interventi. Non è trascurabile invece l'aggiornamento dei dati attraverso Bacula. Di seguito viene mostrato un grafico qualitativo sul guadagno stimato (in termini di tempo).



Tutte le considerazioni fatte fin ora riguardavano la fase di restore, ma con l'utilizzo di VM Explorer è stato introdotto un notevole vantaggio anche nella fase di backup. In precedenza ad ogni backup, i servizi erogati dalle rispettive virtual machine, venivano bloccati per permettere lo spegnimento di queste ultime necessario al salvataggio di tutti i dati. VM Explorer ammette un backup a caldo, cioè senza la necessità di dover bloccare le VM interessate alle operazioni di salvaguardia dati.
Precisazione doverosa riguarda il restore bare metal permesso da Clonezilla. Purtroppo non vi sono software open source in grado di creare immagini eseguibile con la possibilità di installarle su hardware differente dall'originale. In caso di guasto bisognerà provvedere alla sostituzione del pezzo danneggiato con un altro componente del tutto simile all'originale.

Capitolo 9

Test

9.1 Test Clonezilla

Per la prova di collaudo è stato utilizzato un personal computer con queste caratteristiche:

- Intel(R) Pentium(R) Dual CPU
- E2180 @2.00GHz, 2.00GHz
- 896MB RAM
- Microsoft Win xp Professional Versione 2002 SP3

Step1: creazione immagine.
L'applicativo in questione permette la scelta di clonazione di un intero disco, di partizioni oppure la creazione di un immagine, anche in questo caso sia dell'intero disco che solamente una partizione di esso. Per evitare un lavoro oneroso nel creare l'ambiente adatto è stato scelto il backup della partizione contenente il sistema operativo sopra indicato tramite immagine ed è stata salvata sulla seconda partizione che completa il nostro disco. La partizione sorgente è di 106GB di cui 8,23 utilizzati. Il secondo blocco ha una dimensione pari a 30GB. Per ottenere maggiore verosimiltà nel collaudo si avrebbe preferito il backup di una partizione provvista di win server 2003, ciò non è stato fatto alla luce dell'inesistenza di problemi di compatibilità tra i software utilizzati e i sistemi operativi considerati.

Durante la creazione dell'immagine vengo intrapresi vari passaggi riportati di seguito:

- Scegliere l'opzione *clonezilla live* dal menù iniziale;
- Scegliere la lingua preferita;
- Seleziona la mappatura della tastiera della lista delle architetture (qwerty);
- Scegliere layourt tastiera (italia);
- Scegliere mappa tastiera (standard);
- Avvio di clonezilla -> Start_Clonezilla Avvio di Clonezilla;
- Scegliere se salvare o ripristinare immagine oppure se clonare disco/partizione su altro disco/partizione;
- Scegliere dove montare/leggere l'immagine;
- Scegliere la partizione dove salvare l'immagine;
- Scegliere la directory dove verrà salvata l'immagine;
- Modalità esperto;
- Creare un'immagine di una partizione o di un intero disco oppure se montare...;
- Dare nome all'immagine;
- Scegliere la partizione da backupare;
- Scegliere le priorità dei sw per la clonazione: è stata data priorità a ntfsclone lavorando su una partizione ntfs;
- Ora vengono offerte queste opzioni: (vi è la possibilità di scegliere più opzioni ponendo un flag con la barra spazziatrice)

  - il client attende la conferma prima di clonare;
  - clona i dati nascosti tra il MBR e la prima partizione;
  - usa l'output in modalità testo e non TUI/GUI;
  - non forzare l'attivazione DMA sull'HD;
  - se esistono rimuovi i file di page e di ibernazione di win;
  - salta il controllo di integrità ntfs, perfino i settori rovinati (solo ntfsclone);
  - continuo leggendo il prossimo se si verificano errori di lettura dei blocchi del disco;
  - controlla e ripara il file system sorgente prima di salvarlo;
  - genera il checksum MD5 dell'immagine;
  - genera il checksum SHA1 dell'immagine.

- Scegliere l'opzione di compressione :

  - compressione parallela gzip;

- compressione gzip;
- parallela bzip2;
- bzip2;
- lzma (opzione più lenta ma l'immagine più piccola);
- parallela xz;
- xz;
- parallela lzip;
- lzip;
- nessuna compressione.

- Scegliere la dimensione dei file multivolume in cui dividere l'immagine, se non si desidera dividere porre una dimensione abbastanza capiente;
- Scegliere cosa deve fare il client mentre la clonazione termina;

Fatte queste operazioni e atteso il tempo dovuto otteniamo un backup di dimensione pari a 21,7GB ricavati da un totale di 8,7GB di file sorgenti.

Step2: restore immagine.
I passi da seguire per il restore sono del tutto simili alle azioni da intraprendere per la creazione dell'immagine.

- Scegliere l'opzione *clonezilla live* dal menù iniziale;
- Scegliere la lingua;
- Selezionare la mappatura della tastiera dalla lista di architetture;
- Scegliere se avviare clonezilla o fare il login da shell (avvio clonezilla);
- Scegliere salvare un disco/partizione su un'immagine oppure ripristinare immagine su disco/partizione;
- Scegliere in che periferica troviamo l'immagine;
- Scegliere di montare la partizione sulla quale è presente l'immagine, non montare la partizione che si desidera ripristinare;
- Scegliere la directory dove troviamo l'immagine;
- Consigliabile la scelta in modalità principiante;
- Scegliere l'opzione ripristina l'immagine su una partizione;
- Scegliere l'immagine desiderata;
- Scegliere la partizione rispettiva da ripristinare;
- Rispondete "y" a clonezilla..anche alla seconda richiesta seppur insistente.

Tale operazione ha impiegato 10minuti con un rate medio di 1,36GB/min.

9.2 Test VMExplorer

La prova di backup è stata effettuata sull'host 10.11.11.222 sul server ordingtestclone che risponde a queste caratteristiche:

- Virtual hw: 2CPUs, 512MB RAM, 1virtual disks, 1Etherneth Interfaces;
- Stats: Active Mem 384MB, Host Mem 195MB, CPU Usage 1128MHz;
- Disks: [datastore1] ordingtestclone/ordingtestcone.vmdk;

L'operazione di backup ha impiegato 1ora e 36minuti con una velocità media di trasferimento pari a 2MB/s.

VMexplorer ha copiato l'intera configurazione del server ordingtestclone mentre il server stesso era in funzione, dando la possibilità di creare un backup in locale o in rete.
La parte più critica coinvolge il restore della VM, il processo ha impiegato 6ore e 57minuti dando però esito positivo. Ci sono delle accortezze da tenere in considerazione: la procedure crea una nuova cartella di nome "Restore-<nomeOriginario>", questo evita la sovrascrittura dei file consistenti ma necessità di uno spazio di storage pari al doppio dei file che si vogliono salvare, a meno di una cancellazione del setting originale, inoltre si rendono necessarie eventuali modifiche di path tali da permettere al server di puntare il virtual-disk corretto.

9.3 Precisazioni

Il restore intrapreso con VMExplorer è andato a buon fine dopo quasi sette ore di lavoro, questo è sicuramente un tempo non accettabile ma è anche un tempo che non rispecchia la reale prova su campo. Il backup della VM di prova è stato salvato su disco locale della workstation a disposizione causando così un notevole incremento del tempo di spostamento dei singoli file

attraverso la rete interna. In normale situazione il backup verrà posto direttamente sul disco nas ottenendo così un cospicuo guadagno. Come ultima spiaggia, se il tempo di restore non dovesse più che dimezzarsi, si è notato che VMExplorer crea gli stessi file ottenuti dal client VMware con un backup a freddo, questo significa che un semplice spostamento di tali file nella cartella della VM, basta per rendere operativa la macchina stessa. L'operazione di copia è l'azione più ottimizzata nella quale potevamo sperare, con l'unico inconveniente che dev'essere fatta partire a mano o con qualche script creato appositamente.

Bibliografia

[1] LinkToigo, Jon William, 2000. *LinkDisaster recovery planning : strategies for protecting critical information / Jon Eilliam Toigo ; with illustration by Margaret Romao Toigo*, LinkRomao Toigo, Margaret, 2. ed.

[2] Giulio Carducci. *La tutela dei dati nelle aziende e nelle istituzioni. Come integrare gli aspetti giuridici, organizzativi e tecnici per proteggere i dati*, 2a edizione, aggiornata e ampliata 2003, Am / La prima collana di management in Italia.

[3] Garante protezione dati personali *Normativa - 12 luglio 2006* del *Decreto legislativo 30 giugno 2003, n. 196*, Garante Privacy, disponibile all'indirizzo : http://www.garanteprivacy.it/

[4] Garante protezione dati personali *Allegato B* del *Decreto legislativo 30 giugno 2003, n. 196*, Garante Privacy, disponibile all'indirizzo : http://www.garanteprivacy.it/

[5] Informazioni generali su Amanda, wiki e source code. Disponibili all'indirizzo : http://www.amanda.org/

[6] Informazioni generali su Cobian e source code. Disponibili all'indirizzo : http://www.educ.umu.se/ cobian/cobianbackup.htm

[7] Informazioni generali su Icemirror e source code. Disponibili all'indirizzo : http://ice-mirror.software.informer.com/

[8] Informazioni generali su Bacula, wiki e source code. Disponibili all'indirizzo : http://www.bacula.org/en/

[9] Informazioni generali su SyncBack e source code. Disponibili all'indirizzo : http://www.2brightsparks.com/

[10] Informazioni generali su Lifekeeper. Disponibili all'indirizzo : http://www.steeleye.com/it/

[11] Informazioni generali sulla soluzione fornita da Symantec. Disponibili all'indirizzo : http://www.symantec.com/business/backup-exec-system-recovery-server-edition

[12] Informazioni generali sulla soluzione fornita da EMC. Disponibili all'indirizzo : http://www.emc.com/

[13] Informazioni generali sulla soluzione fornita da I.Net. Disponibili all'indirizzo : http://www.inet.it/

[14] Tipologia di backup. Disponibile all'indirizzo : http://technet.microsoft.com/it-it/library/cc784306%28WS.10%29.aspx

Appendice A

Decreto legislativo 30 giugno 2003, n. 196

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, aggiornato in base ai seguenti provvedimenti:

- legge 20 novembre 2009, n. 166 di conversione, con modificazioni, del decreto-legge n. 135 del 25 settembre 2009;
- legge 4 marzo 2009, n. 15
- legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del decreto-legge n. 207 del 30 dicembre 2008;
- legge 6 agosto 2008 n. 133 di conversione, con modificazioni, del decreto-legge 25 giugno 2008, n. 112;
- decreto legislativo 30 maggio 2008, n. 109;
- legge 18 marzo 2008, n. 48 ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno
- legge 26 febbraio 2007, n. 17 di conversione, con modificazioni, del decreto-legge 28 dicembre 2006, n. 300;
- legge 12 luglio 2006, n. 228 di conversione, con modificazioni, del decreto-legge 12 maggio 2006, n. 173;
- legge 23 febbraio 2006, n. 51 di conversione, con modificazioni, del decreto-legge 30 dicembre 2005, n. 273;

- legge 27 gennaio 2006, n. 21 di conversione, con modificazioni, del decreto legge 30 novembre 2005, n. 245;
- decreto legislativo 7 settembre 2005, n. 209;
- legge 31 luglio 2005, n. 155 di conversione, con modificazioni, del decreto-legge 27 luglio 2005, n. 144;
- legge 1 marzo 2005, n. 26 di conversione, con modificazioni, del decreto-legge 30 dicembre 2004, n. 314;
- legge 27 dicembre 2004, n. 306 di conversione, con modificazioni, del decreto-legge 9 novembre 2004, n. 66;
- legge 27 luglio 2004, n. 188 di conversione, con modificazioni, del decreto-legge 24 giugno 2004, n. 158;
- legge 26 maggio 2004, n. 138 di conversione, con modificazioni, del decreto-legge 29 marzo 2004, n. 81;
- decreto legislativo 22 gennaio 2004, n. 42;
- legge 26 febbraio 2004, n. 45 di conversione, con modificazioni, del decreto-legge 24 dicembre 2003, n. 354.

In nota

- legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del decreto decreto legge 30 dicembre 2008, n. 207
- legge 27 febbraio 2008, n. 31 di conversione, con modificazioni, del decreto decreto legge 31 dicembre 2007, n. 248
- legge 31 luglio 2005, n. 155 di conversione, con modificazioni, del decreto-legge 27 luglio 2005, n. 144

A.1 Parte I - Disposizioni generali

A.1.1 Titolo I - Principi generali

Art. 1. Diritto alla protezione dei dati personali

1. Chiunque ha diritto alla protezione dei dati personali che lo riguardano. Le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto ad una funzione pubblica e la relativa valutazione non sono oggetto di protezione della riservatezza personale. (1)

   (1) Così modificato dall'art. 4, comma 9 della legge 4 marzo 2009, n. 15

Art. 2. Finalità

1. Il presente testo unico, di seguito denominato codice, garantisce che il trattamento dei dati personali si svolga 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.

2. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 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.

Art. 3. Principio di necessità nel trattamento dei dati

1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Art. 4. Definizioni

1. Ai fini del presente codice si intende per:

   (a) trattamento, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

(b) dato personale, 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;

(c) dati identificativi, i dati personali che permettono l'identificazione diretta dell'interessato;

(d) dati sensibili, 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;

(e) dati giudiziari, 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 60 e 61 del codice di procedura penale;

(f) 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;

(g) responsabile, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

(h) incaricati, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

(i) interessato, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

(j) comunicazione, il 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;

(k) diffusione, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

(l) dato anonimo, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

(m) blocco, la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

(n) banca di dati, qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

(o) Garante, l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2. Ai fini del presente codice si intende, inoltre, per:

(a) comunicazione elettronica, ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

(b) chiamata, la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

(c) reti di comunicazione elettronica, i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

(d) rete pubblica di comunicazioni, una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

(e) servizio di comunicazione elettronica, i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2,

lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7marzo 2002;

(f) abbonato, qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

(g) utente, qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

(h) dati relativi al traffico, qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

(i) dati relativi all'ubicazione, ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

(j) servizio a valore aggiunto, il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

(k) posta elettronica, messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Ai fini del presente codice si intende, altresì, per:

(a) misure minime, il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

(b) strumenti elettronici, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

(c) autenticazione informatica, l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

(d) credenziali di autenticazione, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

(e) parola chiave, componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

(f) profilo di autorizzazione, l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

(g) sistema di autorizzazione, l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Ai fini del presente codice si intende per:

(a) scopi storici, le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

(b) scopi statistici, le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

(c) scopi scientifici, le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Art. 5. Oggetto ed ambito di applicazione

1. Il presente codice disciplina il 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 Stato.

2. Il presente codice si applica anche al 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, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente 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.

3. Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice

solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31.

Art. 6. Disciplina del trattamento

1. Le disposizioni contenute nella presente Parte si applicano a tutti i trattamenti di dati, salvo quanto previsto, in relazione ad alcuni trattamenti, dalle disposizioni integrative o modificative della Parte II.

A.1.2 Titolo II - Diritti dell'interessato

Art. 7. Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto 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.

2. L'interessato ha diritto di ottenere l'indicazione:

   (a) dell'origine dei dati personali;

   (b) dell'origine dei dati personali;

   (c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

   (d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

   (e) dei soggetti o delle 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.

3. L'interessato ha diritto di ottenere:

   (a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

   (b) la cancellazione, la trasformazione in forma anonima o il blocco 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;

(c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato 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.

Art. 8. Esercizio dei diritti

1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.

2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, 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;

   (c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;

   (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;

(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.

3. Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f) provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.

4. L'esercizio dei diritti di cui all'articolo 7, 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.

Art. 9. Modalità di esercizio

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. 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.

2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.

3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

4. 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. 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.

5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

Art. 10. Riscontro all'interessato

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:

   (a) 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;

   (b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se 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.

4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

A.1.3 Titolo III - Regole generali per il trattamento dei dati

Capo I - Regole per tutti i trattamenti

Art. 11. Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:
   (a) trattati in modo lecito e secondo correttezza;
   (b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
   (c) esatti e, se necessario, aggiornati;
   (d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
   (e) 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.
2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Art. 12. Codici di deontologia e di buona condotta

1. 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.
2. 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.
3. 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.

4. 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.

Art. 13. Informativa(1)

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
   (a) le finalità e le modalità del trattamento cui sono destinati i dati;
   (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 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;
   (e) i diritti di cui all'articolo 7;
   (f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente 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.

3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.

4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

5. La disposizione di cui al comma 4 non si applica quando:

   (a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

   (b) 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;

   (c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

(1) La legge 27 febbraio 2009, n. 14, in sede di conversione con modificazioni del decreto-legge 30 dicembre 2008, n. 207, vi ha aggiunto il seguente comma: ***Art. 44 - Disposizioni in materia di tutela della riservatezza*** *[...]*
1-bis - I dati personali presenti nelle banche dati costituite sulla base di elenchi telefonici formati prima del 1° agosto 2005 sono lecitamente utilizzabili per fini promozionali sino al 31 dicembre 2009, anche in deroga agli articoli 13 e 23 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, dai soli titolari del trattamento che hanno provveduto a costituire dette banche dati prima del 1° agosto 2005.
[...]
(2) La Legge 20 novembre 2009, n. 166, in sede di conversione con modificazioni del decreto-legge 25 settembre 2009 n. 135, ha stabilito che all'articolo 44, comma 1-bis, del decreto-legge 30 dicembre 2008, n. 207, convertito, con modificazioni, dalla legge 27 febbraio 2009 n. 14, le parole: sino al 31 dicembre 2009 sono sostituite dalle seguenti: sino al termine di sei mesi successivi alla data di entrata in vigore della legge di conversione del decreto-legge 25 settembre 2009, n. 135.

Art. 14. Definizione di profili e della personalità dell'interessato

1. 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.

2. 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.

Art. 15. Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Art. 16. Cessazione del trattamento

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:

   (a) distrutti;

   (b) ceduti ad altro titolare, purchè destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;

   (c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;

   (d) 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.

2. La cessione dei dati in violazione di quanto previsto dal comma 1, lettera b), o di altre disposizioni rilevanti in materia di trattamento dei dati personali è priva di effetti.

Art. 17. Trattamento che presenta rischi specifici

1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta 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, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante 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.

Capo II - Regole ulteriori per i soggetti pubblici

Art. 18. Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici

1. Le disposizioni del presente capo riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici.

2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

3. Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.

4. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato.

5. Si osservano le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione.

Art. 19. Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari

1. Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente

2. 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.

3. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Art. 20. Principi applicabili al trattamento di dati sensibili

1. Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

2. 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.

3. 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 a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2.

4. L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente.

Art. 21. Principi applicabili al trattamento di dati giudiziari

1. Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

2. Le disposizioni di cui all'articolo 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari.

Art. 22. Principi applicabili al trattamento di dati sensibili e giudiziari

1. I soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

2. Nel fornire l'informativa di cui all'articolo 13 i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

3. I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

4. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.

5. In applicazione dell'articolo 11, comma 1, lettere c), d) ed e), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con 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

7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per 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.

10. I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi.

11. In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.

12. Le disposizioni di cui al presente articolo 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.

Capo III - Regole ulteriori per privati ed enti pubblici economici

Art. 23. Consenso(1)

1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.

4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

(1) La legge 27 febbraio 2009, n. 14, in sede di conversione con modificazioni del decreto-legge 30 dicembre 2008, n. 207, vi ha aggiunto il seguente comma:
***Art. 44 - Disposizioni in materia di tutela della riservatezza** [...]*
1-bis - I dati personali presenti nelle banche dati costituite sulla base di elenchi telefonici formati prima del 1° agosto 2005 sono lecitamente utilizzabili per fini promozionali sino al 31 dicembre 2009, anche in deroga agli articoli 13 e 23 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, dai soli titolari del trattamento che hanno provveduto a costituire dette banche dati prima del 1° agosto 2005.
[...]
(2) La Legge 20 novembre 2009, n. 166, in sede di conversione con modificazioni del decreto-legge 25 settembre 2009 n. 135, ha stabilito che all'articolo 44, comma 1-bis, del decreto-legge 30 dicembre 2008, n. 207, convertito, con modificazioni, dalla legge 27 febbraio 2009 n. 14, le parole: sino al 31 dicembre 2009 sono sostituite dalle seguenti: sino al termine di sei mesi successivi alla data di entrata in vigore della legge di conversione del decreto-legge 25 settembre 2009, n. 135.

Art. 24. Casi nei quali può essere effettuato il trattamento senza consenso

1. Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:

   (a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

   (b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;

(c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;

(d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

(e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

(f) con esclusione della diffusione, è necessario 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, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

(g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;

(h) con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

(i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per

esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati.

Art. 25. Divieti di comunicazione e diffusione

1. La comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dal Garante o dall'autorità giudiziaria:
   (a) in riferimento a dati personali dei quali è stata ordinata la cancellazione, ovvero quando è decorso il periodo di tempo indicato nell'articolo 11, comma 1, lettera e);
   (b) per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta.
2. È fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'articolo 58, comma 2, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

Art. 26. Garanzie per i dati sensibili

1. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti.
2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.
3. Il comma 1 non si applica al trattamento:
   (a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa

hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

(b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria.

4. I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:

(a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

(b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

(c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i

dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

(d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111.

5. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

Art. 27. Garanzie per i dati giudiziari

1. Il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

A.1.4 Titolo IV - Soggetti che effettuano il trattamento

Art. 28. Titolare del trattamento

1. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Art. 29. Responsabile del trattamento

1. Il responsabile è designato dal titolare facoltativamente.

2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

Art. 30. Incaricati del trattamento

1. 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.

2. La designazione è effettuata per iscritto e individua 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.

A.1.5 Titolo V - Sicurezza dei dati e dei sistemi

Capo I - Misure di sicurezza

Art. 31. Obblighi di sicurezza

1. 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.

Art. 32. Particolari titolari

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita.

2. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi dei commi 1 e 2, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni.

Capo II - Misure minime di sicurezza

Art. 33. Misure minime

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34. Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

   (a) autenticazione informatica;

   (b) adozione di procedure di gestione delle credenziali di autenticazione;

(c) utilizzazione di un sistema di autorizzazione;

(d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

(e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

(f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

(g) tenuta di un aggiornato documento programmatico sulla sicurezza;

(h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

1-bis. Per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale, la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo di autocertificazione, resa dal titolare del trattamento ai sensi dell'articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte. In relazione a tali trattamenti, nonché a trattamenti comunque effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante, sentito il Ministro per la semplificazione normativa, individua con proprio provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico di cui all'Allegato B) in ordine all'adozione delle misure minime di cui al comma 1.

Art. 35. Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

   (a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

(b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

(c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Art. 36. Adeguamento

1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie e il Ministro per la semplificazione normativa, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

A.1.6 Titolo VI - Adempimenti

Art. 37. Notificazione del trattamento

1. Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:

   (a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;

   (b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;

   (c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;

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

(e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;

(f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

1-bis. La notificazione relativa al trattamento dei dati di cui al comma 1 non è dovuta se relativa all'attività dei medici di famiglia e dei pediatri di libera scelta, in quanto tale funzione è tipica del loro rapporto professionale con il Servizio sanitario nazionale.

2. Il Garante può individuare altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali, con proprio provvedimento adottato anche ai sensi dell'articolo 17. Con analogo provvedimento pubblicato sulla Gazzetta Ufficiale della Repubblica italiana il Garante può anche individuare, nell'ambito dei trattamenti di cui al comma 1, eventuali trattamenti non suscettibili di recare detto pregiudizio e pertanto sottratti all'obbligo di notificazione.

3. La notificazione è effettuata con unico atto anche quando il trattamento comporta il trasferimento all'estero dei dati.

4. Il Garante inserisce le notificazioni ricevute in un registro dei trattamenti accessibile a chiunque e determina le modalità per la sua consultazione gratuita per via telematica, anche mediante convenzioni con soggetti pubblici o presso il proprio Ufficio. Le notizie accessibili tramite la consultazione del registro possono essere trattate per esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali.

Art. 38. Modalità di notificazione

1. La notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare, e può anche riguardare uno o più trattamenti con finalità correlate.

2. La notificazione è validamente effettuata solo se è trasmessa attraverso il sito del Garante, utilizzando l'apposito modello, che contiene la richiesta di fornire tutte e soltanto le seguenti informazioni:

(a) le coordinate identificative del titolare del trattamento e, eventualmente, del suo rappresentante, nonché le modalità per individuare il responsabile del trattamento se designato;

(b) la o le finalità del trattamento;

(c) una descrizione della o delle categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime;

(d) i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;

(e) i trasferimenti di dati previsti verso Paesi terzi;

(f) una descrizione generale che permetta di valutare in via preliminare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento.

3. Il Garante favorisce la disponibilità del modello per via telematica e la notificazione anche attraverso convenzioni stipulate con soggetti autorizzati in base alla normativa vigente, anche presso associazioni di categoria e ordini professionali.

4. Una nuova notificazione è richiesta solo anteriormente alla cessazione del trattamento o al mutamento di taluno degli elementi da indicare nella notificazione medesima.

5. Il Garante può individuare altro idoneo sistema per la notificazione in riferimento a nuove soluzioni tecnologiche previste dalla normativa vigente.

6. Il titolare del trattamento che non è tenuto alla notificazione al Garante ai sensi dell'articolo 37 fornisce le notizie contenute nel modello di cui al comma 2 a chi ne fa richiesta, salvo che il trattamento riguardi pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

Art. 39. Obblighi di comunicazione

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

(a) comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento, effettuata in qualunque forma anche mediante convenzione;

(b) trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria di cui all'articolo 110, comma 1, primo periodo.

2. I trattamenti oggetto di comunicazione ai sensi del comma 1 possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione salvo diversa determinazione anche successiva del Garante

3. La comunicazione di cui al comma 1 è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa a quest'ultimo per via telematica osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento di cui all'articolo 38, comma 2, oppure mediante telefax o lettera raccomandata.

Art. 40. Autorizzazioni generali

1. 1. Le disposizioni del presente codice che prevedono un'autorizzazione del Garante sono applicate anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti, pubblicate nella Gazzetta Ufficiale della Repubblica italiana.

Art. 41. Richieste di autorizzazione

1. Il titolare del trattamento che rientra nell'ambito di applicazione di un'autorizzazione rilasciata ai sensi dell'articolo 40 non è tenuto a presentare al Garante una richiesta di autorizzazione se il trattamento che intende effettuare è conforme alle relative prescrizioni.

2. Se una richiesta di autorizzazione riguarda un trattamento autorizzato ai sensi dell'articolo 40 il Garante può provvedere comunque sulla richiesta se le specifiche modalità del trattamento lo giustificano.

3. L'eventuale richiesta di autorizzazione è formulata utilizzando esclusivamente il modello predisposto e reso disponibile dal Garante e trasmessa a quest'ultimo per via telematica, osservando le modalità di sottoscrizione e conferma del ricevimento di cui all'articolo 38, comma 2. La medesima richiesta e l'autorizzazione possono essere trasmesse anche mediante telefax o lettera raccomandata.

4. Se il richiedente è invitato dal Garante a fornire informazioni o ad esibire documenti, il termine di quarantacinque giorni di cui all'articolo

26, comma 2, decorre dalla data di scadenza del termine fissato per l'adempimento richiesto.

5. In presenza di particolari circostanze, il Garante può rilasciare un'autorizzazione provvisoria a tempo determinato.

A.1.7 Titolo VII - Trasferimento dei dati all'estero

Art. 42. Trasferimenti all'interno dell'Unione europea

1. 1. Le disposizioni del presente codice non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione, in conformità allo stesso codice, di eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni.

Art. 43. Trasferimenti consentiti in Paesi terzi

1. Il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, se diretto verso un Paese non appartenente all'Unione europea è consentito quando:

   (a) l'interessato ha manifestato il proprio consenso espresso o, se si tratta di dati sensibili, in forma scritta;

   (b) è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;

   (c) è necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento o, se il trasferimento riguarda dati sensibili o giudiziari, specificato o individuato ai sensi degli articoli 20 e 21;

   (d) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la

potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

(e) è necessario 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 trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

(f) è effettuato in accoglimento di una richiesta di accesso ai documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia;

(g) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati;

(h) il trattamento concerne dati riguardanti persone giuridiche, enti o associazioni.

Art. 44. Altri trasferimenti consentiti

1. Il trasferimento di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è altresì consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato:

   (a) individuate dal Garante anche in relazione a garanzie prestate con un contratto o mediante regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo. L'interessato può far valere i propri diritti nel territorio dello Stato, in base al presente codice, anche in ordine all'inosservanza delle garanzie medesime;

   (b) individuate con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, con le quali la Commissione

europea constata che un Paese non appartenente all'Unione europea garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti.

Art. 45. Trasferimenti vietati

1. Fuori dei casi di cui agli articoli 43 e 44, il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato. Sono valutate anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza.

A.2 Parte II - Disposizioni relative a specifici settori

A.2.1 Titolo I - Trattamenti in ambito giudiziario

Capo I - Profili generali

Art. 46. Titolari dei trattamenti

1. Gli uffici giudiziari di ogni ordine e grado, il Consiglio superiore della magistratura, gli altri organi di autogoverno e il Ministero della giustizia sono titolari dei trattamenti di dati personali relativi alle rispettive attribuzioni conferite per legge o regolamento.

2. Con decreto del Ministro della giustizia sono individuati, nell'allegato C) al presente codice, i trattamenti non occasionali di cui al comma 1 effettuati con strumenti elettronici, relativamente a banche di dati centrali od oggetto di interconnessione tra più uffici o titolari. I provvedimenti con cui il Consiglio superiore della magistratura e gli altri organi di autogoverno di cui al comma 1 individuano i medesimi trattamenti da essi effettuati sono riportati nell'allegato C) con decreto del Ministro della giustizia.

Art. 47. Trattamenti per ragioni di giustizia

1. In caso di trattamento di dati personali effettuato presso uffici giudiziari di ogni ordine e grado, presso il Consiglio superiore della magistratura, gli altri organi di autogoverno e il Ministero della giustizia, non si applicano, se il trattamento è effettuato per ragioni di giustizia, le seguenti disposizioni del codice:

   (a) articoli 9, 10, 12, 13 e 16, da 18 a 22, 37, 38, commi da 1 a 5, e da 39 a 45;

   (b) articoli da 145 a 151.

2. Agli effetti del presente codice si intendono effettuati per ragioni di giustizia i trattamenti di dati personali direttamente correlati alla trattazione giudiziaria di affari e di controversie, o che, in materia di trattamento giuridico ed economico del personale di magistratura, hanno una diretta incidenza sulla funzione giurisdizionale, nonché le attività ispettive su uffici giudiziari. Le medesime ragioni di giustizia non ricorrono per l'ordinaria attività amministrativo-gestionale di personale, mezzi o strutture, quando non è pregiudicata la segretezza di atti direttamente connessi alla predetta trattazione.

Art. 48. Banche di dati di uffici giudiziari

1. Nei casi in cui l'autorità giudiziaria di ogni ordine e grado può acquisire in conformità alle vigenti disposizioni processuali dati, informazioni, atti e documenti da soggetti pubblici, l'acquisizione può essere effettuata anche per via telematica. A tale fine gli uffici giudiziari possono avvalersi delle convenzioni-tipo stipulate dal Ministero della giustizia con soggetti pubblici, volte ad agevolare la consultazione da parte dei medesimi uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei principi di cui agli articoli 3 e 11 del presente codice.

Art. 49. Disposizioni di attuazione

1. Con decreto del Ministro della giustizia sono adottate, anche ad integrazione del decreto del Ministro di grazia e giustizia 30 settembre 1989, n. 334, le disposizioni regolamentari necessarie per l'attuazione dei principi del presente codice nella materia penale e civile.

Capo II - Minori

Art. 50. Notizie o immagini relative a minori

1. Il divieto di cui all'articolo 13 del decreto del Presidente della Repubblica 22 settembre 1988, n. 448, di pubblicazione e divulgazione con qualsiasi mezzo di notizie o immagini idonee a consentire l'identificazione di un minore si osserva anche in caso di coinvolgimento a qualunque titolo del minore in procedimenti giudiziari in materie diverse da quella penale.

Capo III - Informatica giuridica

Art. 51. Principi generali

1. Fermo restando quanto previsto dalle disposizioni processuali concernenti la visione e il rilascio di estratti e di copie di atti e documenti, i dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado sono resi accessibili a chi vi abbia interesse anche mediante reti di comunicazione elettronica, ivi compreso il sito istituzionale della medesima autorità nella rete Internet.

2. Le sentenze e le altre decisioni dell'autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet, osservando le cautele previste dal presente capo.

Art. 52. Dati identificativi degli interessati

1. Fermo restando quanto previsto dalle disposizioni concernenti la redazione e il contenuto di sentenze e di altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado, l'interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, per finalità di informazione giuridica su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento.

2. Sulla richiesta di cui al comma 1 provvede in calce con decreto, senza ulteriori formalità, l'autorità che pronuncia la sentenza o adotta il provvedimento. La medesima autorità può disporre d'ufficio che sia apposta l'annotazione di cui al comma 1, a tutela dei diritti o della dignità degli interessati.

3. Nei casi di cui ai commi 1 e 2, all'atto del deposito della sentenza o provvedimento, la cancelleria o segreteria vi appone e sottoscrive anche con timbro la seguente annotazione, recante l'indicazione degli estremi del presente articolo: In caso di diffusione omettere le generalità e gli altri dati identificativi di ....

4. In caso di diffusione anche da parte di terzi di sentenze o di altri provvedimenti recanti l'annotazione di cui al comma 2, o delle relative massime giuridiche, è omessa l'indicazione delle generalità e degli altri dati identificativi dell'interessato.

5. Fermo restando quanto previsto dall'articolo 734-bis del codice penale relativamente alle persone offese da atti di violenza sessuale, chiunque diffonde sentenze o altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado è tenuto ad omettere in ogni caso, anche in mancanza dell'annotazione di cui al comma 2, le generalità, altri dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità di minori, oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone.

6. Le disposizioni di cui al presente articolo si applicano anche in caso di deposito di lodo ai sensi dell'articolo 825 del codice di procedura civile. La parte può formulare agli arbitri la richiesta di cui al comma 1 prima della pronuncia del lodo e gli arbitri appongono sul lodo l'annotazione di cui al comma 3, anche ai sensi del comma 2. Il collegio arbitrale costituito presso la camera arbitrale per i lavori pubblici ai sensi dell'articolo 32 della legge 11 febbraio 1994, n. 109, provvede in modo analogo in caso di richiesta di una parte.

7. Fuori dei casi indicati nel presente articolo è ammessa la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali.

A.2.2 Titolo II - Trattamenti da parte di forze di polizia

Capo I - Profili generali

Art. 53. Ambito applicativo e titolari dei trattamenti

1. Al trattamento di dati personali effettuato dal Centro elaborazione dati del Dipartimento di pubblica sicurezza o da forze di polizia sui dati destinati a confluirvi in base alla legge, ovvero da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento, non si applicano le seguenti disposizioni del codice:
   (a) articoli 9, 10, 12, 13 e 16, da 18 a 22, 37, 38, commi da 1 a 5, e da 39 a 45;
   (b) articoli da 145 a 151.
2. Con decreto del Ministro dell'interno sono individuati, nell'allegato C) al presente codice, i trattamenti non occasionali di cui al comma 1 effettuati con strumenti elettronici, e i relativi titolari.

Art. 54. Modalità di trattamento e flussi di dati

1. Nei casi in cui le autorità di pubblica sicurezza o le forze di polizia possono acquisire in conformità alle vigenti disposizioni di legge o di regolamento dati, informazioni, atti e documenti da altri soggetti, l'acquisizione può essere effettuata anche per via telematica. A tal fine gli organi o uffici interessati possono avvalersi di convenzioni volte ad agevolare la consultazione da parte dei medesimi organi o uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei principi di cui agli articoli 3 e 11. Le convenzioni-tipo sono adottate dal Ministero dell'interno, su conforme parere del Garante, e stabiliscono le modalità dei collegamenti e degli accessi anche al fine di assicurare l'accesso selettivo ai soli dati necessari al perseguimento delle finalità di cui all'articolo 53.
2. I dati trattati per le finalità di cui al medesimo articolo 53 sono conservati separatamente da quelli registrati per finalità amministrative che non richiedono il loro utilizzo.
3. Fermo restando quanto previsto dall'articolo 11, il Centro elaborazioni dati di cui all'articolo 53 assicura l'aggiornamento periodico e la pertinenza e non eccedenza dei dati personali trattati anche attraverso

interrogazioni autorizzate del casellario giudiziale e del casellario dei carichi pendenti del Ministero della giustizia di cui al decreto del Presidente della Repubblica 14 novembre 2002, n. 313, o di altre banche di dati di forze di polizia, necessarie per le finalità di cui all'articolo 53.

4. Gli organi, uffici e comandi di polizia verificano periodicamente i requisiti di cui all'articolo 11 in riferimento ai dati trattati anche senza l'ausilio di strumenti elettronici, e provvedono al loro aggiornamento anche sulla base delle procedure adottate dal Centro elaborazioni dati ai sensi del comma 3, o, per i trattamenti effettuati senza l'ausilio di strumenti elettronici, mediante annotazioni o integrazioni dei documenti che li contengono.

Art. 55. Particolari tecnologie

1. Il trattamento di dati personali che implica maggiori rischi di un danno all'interessato, con particolare riguardo a banche di dati genetici o biometrici, a tecniche basate su dati relativi all'ubicazione, a banche di dati basate su particolari tecniche di elaborazione delle informazioni e all'introduzione di particolari tecnologie, è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17 sulla base di preventiva comunicazione ai sensi dell'articolo 39.

Art. 56. Tutela dell'interessato

1. Le disposizioni di cui all'articolo 10, commi 3, 4 e 5, della legge 1 aprile 1981, n. 121, e successive modificazioni, si applicano anche, oltre che ai dati destinati a confluire nel Centro elaborazioni dati di cui all'articolo 53, a dati trattati con l'ausilio di strumenti elettronici da organi, uffici o comandi di polizia.

Art. 57. Disposizioni di attuazione

1. 1. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, su proposta del Ministro dell'interno, di concerto con il Ministro della giustizia, sono individuate le modalità di attuazione dei principi del presente codice relativamente al trattamento dei dati effettuato per le finalità di cui all'articolo 53 dal Centro

elaborazioni dati e da organi, uffici o comandi di polizia, anche ad integrazione e modifica del decreto del Presidente della Repubblica 3 maggio 1982, n. 378, e in attuazione della Raccomandazione R (87) 15 del Consiglio d'Europa del 17 settembre 1987, e successive modificazioni. Le modalità sono individuate con particolare riguardo:

(a) al principio secondo cui la raccolta dei dati è correlata alla specifica finalità perseguita, in relazione alla prevenzione di un pericolo concreto o alla repressione di reati, in particolare per quanto riguarda i trattamenti effettuati per finalità di analisi;

(b) all'aggiornamento periodico dei dati, anche relativi a valutazioni effettuate in base alla legge, alle diverse modalità relative ai dati trattati senza l'ausilio di strumenti elettronici e alle modalità per rendere conoscibili gli aggiornamenti da parte di altri organi e uffici cui i dati sono stati in precedenza comunicati;

(c) ai presupposti per effettuare trattamenti per esigenze temporanee o collegati a situazioni particolari, anche ai fini della verifica dei requisiti dei dati ai sensi dell'articolo 11, dell'individuazione delle categorie di interessati e della conservazione separata da altri dati che non richiedono il loro utilizzo;

(d) all'individuazione di specifici termini di conservazione dei dati in relazione alla natura dei dati o agli strumenti utilizzati per il loro trattamento, nonché alla tipologia dei procedimenti nell'ambito dei quali essi sono trattati o i provvedimenti sono adottati;

(e) alla comunicazione ad altri soggetti, anche all'estero o per l'esercizio di un diritto o di un interesse legittimo, e alla loro diffusione, ove necessaria in conformità alla legge;

(f) all'uso di particolari tecniche di elaborazione e di ricerca delle informazioni, anche mediante il ricorso a sistemi di indice.

A.2.3 Titolo III - Difesa e sicurezza dello Stato

Capo I - Profili generali

Art. 58. Disposizioni applicabili

1. Ai trattamenti effettuati dagli organismi di cui agli articoli 3, 4 e 6 della legge 24 ottobre 1977, n. 801, ovvero sui dati coperti da segreto di Stato ai sensi dell'articolo 12 della medesima legge, le disposizioni

del presente codice si applicano limitatamente a quelle previste negli articoli da 1 a 6, 11, 14, 15, 31, 33, 58, 154, 160 e 169.

2. Ai trattamenti effettuati da soggetti pubblici per finalità di difesa o di sicurezza dello Stato, in base ad espresse disposizioni di legge che prevedano specificamente il trattamento, le disposizioni del presente codice si applicano limitatamente a quelle indicate nel comma 1, nonché alle disposizioni di cui agli articoli 37, 38 e 163.

3. Le misure di sicurezza relative ai dati trattati dagli organismi di cui al comma 1 sono stabilite e periodicamente aggiornate con decreto del Presidente del Consiglio dei ministri, con l'osservanza delle norme che regolano la materia.

4. Con decreto del Presidente del Consiglio dei ministri sono individuate le modalità di applicazione delle disposizioni applicabili del presente codice in riferimento alle tipologie di dati, di interessati, di operazioni di trattamento eseguibili e di incaricati, anche in relazione all'aggiornamento e alla conservazione.

A.2.4 Titolo IV - Trattamenti in ambito pubblico

Capo I - Accesso a documenti amministrativi

Art. 59. Accesso a documenti amministrativi

1. Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

Art. 60. Dati idonei a rivelare lo stato di salute e la vita sessuale

1. Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se 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.

Capo II - Registri pubblici e albi professionali

Art. 61. Utilizzazione di dati pubblici

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici, anche individuando i casi in cui deve essere indicata la fonte di acquisizione dei dati e prevedendo garanzie appropriate per l'associazione di dati provenienti da più archivi, tenendo presente quanto previsto dalla Raccomandazione R (91) 10 del Consiglio d'Europa in relazione all'articolo 11.

2. Agli effetti dell'applicazione del presente codice i dati personali diversi da quelli sensibili o giudiziari, che devono essere inseriti in un albo professionale in conformità alla legge o ad un regolamento, possono essere comunicati a soggetti pubblici e privati o diffusi, ai sensi dell'articolo 19, commi 2 e 3, anche mediante reti di comunicazione elettronica. Può essere altresì menzionata l'esistenza di provvedimenti che dispongono la sospensione o che incidono sull'esercizio della professione.

3. L'ordine o collegio professionale può, a richiesta della persona iscritta nell'albo che vi ha interesse, integrare i dati di cui al comma 2 con ulteriori dati pertinenti e non eccedenti in relazione all'attività professionale.

4. A richiesta dell'interessato l'ordine o collegio professionale può altresì fornire a terzi notizie o informazioni relative, in particolare, a speciali qualificazioni professionali non menzionate nell'albo, ovvero alla disponibilità ad assumere incarichi o a ricevere materiale informativo a carattere scientifico inerente anche a convegni o seminari.

Capo III - Stato civile, anagrafi e liste elettorali

Art. 62. Dati sensibili e giudiziari

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità relative alla tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché al rilascio di documenti di riconoscimento o al cambiamento delle generalità.

Art. 63. Consultazione di atti

1. Gli atti dello stato civile conservati negli Archivi di Stato sono consultabili nei limiti previsti dall'articolo 107 del decreto legislativo 29 ottobre 1999, n. 490.

Capo IV - Finalità di rilevante interesse pubblico

Art. 64. Cittadinanza, immigrazione e condizione dello straniero

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di cittadinanza, di immigrazione, di asilo, di condizione dello straniero e del profugo e sullo stato di rifugiato.

2. Nell'ambito delle finalità di cui al comma 1 è ammesso, in particolare, il trattamento dei dati sensibili e giudiziari indispensabili:

   (a) al rilascio e al rinnovo di visti, permessi, attestazioni, autorizzazioni e documenti anche sanitari;

   (b) al riconoscimento del diritto di asilo o dello stato di rifugiato, o all'applicazione della protezione temporanea e di altri istituti o misure di carattere umanitario, ovvero all'attuazione di obblighi di legge in materia di politiche migratorie;

   (c) in relazione agli obblighi dei datori di lavoro e dei lavoratori, ai ricongiungimenti, all'applicazione delle norme vigenti in materia di istruzione e di alloggio, alla partecipazione alla vita pubblica e all'integrazione sociale.

3. Il presente articolo non si applica ai trattamenti di dati sensibili e giudiziari effettuati in esecuzione degli accordi e convenzioni di cui all'articolo 154, comma 2, lettere a) e b), o comunque effettuati per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione dei reati, in base ad espressa disposizione di legge che prevede specificamente il trattamento.

Art. 65. Diritti politici e pubblicità dell'attività di organi

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di:

   (a) elettorato attivo e passivo e di esercizio di altri diritti politici, nel rispetto della segretezza del voto, nonché di esercizio del mandato degli organi rappresentativi o di tenuta degli elenchi dei giudici popolari;

   (b) documentazione dell'attività istituzionale di organi pubblici.

2. I trattamenti dei dati sensibili e giudiziari per le finalità di cui al comma 1 sono consentiti per eseguire specifici compiti previsti da leggi o da regolamenti fra i quali, in particolare, quelli concernenti:

   (a) lo svolgimento di consultazioni elettorali e la verifica della relativa regolarità;

   (b) le richieste di referendum, le relative consultazioni e la verifica delle relative regolarità;

   (c) l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, o di rimozione o sospensione da cariche pubbliche, ovvero di sospensione o di scioglimento degli organi;

   (d) l'esame di segnalazioni, petizioni, appelli e di proposte di legge di iniziativa popolare, l'attività di commissioni di inchiesta, il rapporto con gruppi politici;

   (e) la designazione e la nomina di rappresentanti in commissioni, enti e uffici.

3. Ai fini del presente articolo, è consentita la diffusione dei dati sensibili e giudiziari per le finalità di cui al comma 1, lettera a), in particolare con riguardo alle sottoscrizioni di liste, alla presentazione delle candidature, agli incarichi in organizzazioni o associazioni politiche, alle cariche istituzionali e agli organi eletti.

4. Ai fini del presente articolo, in particolare, è consentito il trattamento di dati sensibili e giudiziari indispensabili:

   (a) per la redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;

(b) per l'esclusivo svolgimento di una funzione di controllo, di indirizzo politico o di sindacato ispettivo e per l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo.

5. I dati sensibili e giudiziari trattati per le finalità di cui al comma 1 possono essere comunicati e diffusi nelle forme previste dai rispettivi ordinamenti. Non è comunque consentita la divulgazione dei dati sensibili e giudiziari che non risultano indispensabili per assicurare il rispetto del principio di pubblicità dell'attività istituzionale, fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute.

Art. 66. Materia tributaria e doganale

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia di tributi, in relazione ai contribuenti, ai sostituti e ai responsabili di imposta, nonché in materia di deduzioni e detrazioni e per l'applicazione delle disposizioni la cui esecuzione è affidata alle dogane.

2. Si considerano inoltre di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le attività dirette, in materia di imposte, alla prevenzione e repressione delle violazioni degli obblighi e alla adozione dei provvedimenti previsti da leggi, regolamenti o dalla normativa comunitaria, nonché al controllo e alla esecuzione forzata dell'esatto adempimento di tali obblighi, alla effettuazione dei rimborsi, alla destinazione di quote d'imposta, e quelle dirette alla gestione ed alienazione di immobili statali, all'inventario e alla qualificazione degli immobili e alla conservazione dei registri immobiliari.

Art. 67. Attività di controllo e ispettive

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di:

(a) verifica della legittimità, del buon andamento, dell'imparzialità dell'attività amministrativa, nonché della rispondenza di detta attività a requisiti di razionalità, economicità, efficienza ed efficacia

per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti;

(b) accertamento, nei limiti delle finalità istituzionali, con riferimento a dati sensibili e giudiziari relativi ad esposti e petizioni, ovvero ad atti di controllo o di sindacato ispettivo di cui all'articolo 65, comma 4.

Art. 68. Benefici economici ed abilitazioni

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni.

2. Si intendono ricompresi fra i trattamenti regolati dal presente articolo anche quelli indispensabili in relazione:

   (a) alle comunicazioni, certificazioni ed informazioni previste dalla normativa antimafia;

   (b) alle elargizioni di contributi previsti dalla normativa in materia di usura e di vittime di richieste estorsive;

   (c) alla corresponsione delle pensioni di guerra o al riconoscimento di benefici in favore di perseguitati politici e di internati in campo di sterminio e di loro congiunti;

   (d) al riconoscimento di benefici connessi all'invalidità civile;

   (e) alla concessione di contributi in materia di formazione professionale;

   (f) alla concessione di contributi, finanziamenti, elargizioni ed altri benefici previsti dalla legge, dai regolamenti o dalla normativa comunitaria, anche in favore di associazioni, fondazioni ed enti;

   (g) al riconoscimento di esoneri, agevolazioni o riduzioni tariffarie o economiche, franchigie, o al rilascio di concessioni anche radiotelevisive, licenze, autorizzazioni, iscrizioni ed altri titoli abilitativi previsti dalla legge, da un regolamento o dalla normativa comunitaria.

3. Il trattamento può comprendere la diffusione nei soli casi in cui ciò è indispensabile per la trasparenza delle attività indicate nel presente

articolo, in conformità alle leggi, e per finalità di vigilanza e di controllo conseguenti alle attività medesime, fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute.

Art. 69. Onorificenze, ricompense e riconoscimenti

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di conferimento di onorificenze e ricompense, di riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, di accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché di rilascio e revoca di autorizzazioni o abilitazioni, di concessione di patrocini, patronati e premi di rappresentanza, di adesione a comitati d'onore e di ammissione a cerimonie ed incontri istituzionali.

Art. 70. Volontariato e obiezione di coscienza

1. Si considerano di rilevante interesse pubblico, ai sensi dell'articoli 20 e 21, le finalità di applicazione della disciplina in materia di rapporti tra i soggetti pubblici e le organizzazioni di volontariato, in particolare per quanto riguarda l'elargizione di contributi finalizzati al loro sostegno, la tenuta di registri generali delle medesime organizzazioni e la cooperazione internazionale.

2. Si considerano, altresì, di rilevante interesse pubblico le finalità di applicazione della legge 8 luglio 1998, n. 230, e delle altre disposizioni di legge in materia di obiezione di coscienza.

Art. 71. Attività sanzionatorie e di tutela

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità:

   (a) di applicazione delle norme in materia di sanzioni amministrative e ricorsi;

   (b) volte a far valere il diritto di difesa in sede amministrativa o giudiziaria, anche da parte di un terzo, anche ai sensi dell'articolo 391-quater del codice di procedura penale, o direttamente

connesse alla riparazione di un errore giudiziario o in caso di violazione del termine ragionevole del processo o di un'ingiusta restrizione della libertà personale.

2. Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se il diritto da far valere o difendere, di cui alla lettera b) del comma 1, è di rango almeno pari a quello dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Art. 72. Rapporti con enti di culto

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità relative allo svolgimento dei rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose.

Art. 73. Altre finalità in ambito amministrativo e sociale

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, nell'ambito delle attività che la legge demanda ad un soggetto pubblico, le finalità socio-assistenziali, con particolare riferimento a:

   (a) interventi di sostegno psico-sociale e di formazione in favore di giovani o di altri soggetti che versano in condizioni di disagio sociale, economico o familiare;

   (b) nterventi anche di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto;

   (c) assistenza nei confronti di minori, anche in relazione a vicende giudiziarie;

   (d) indagini psico-sociali relative a provvedimenti di adozione anche internazionale;

   (e) compiti di vigilanza per affidamenti temporanei;

   (f) iniziative di vigilanza e di sostegno in riferimento al soggiorno di nomadi;

   (g) interventi in tema di barriere architettoniche.

2. Si considerano, altresì, di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, nell'ambito delle attività che la legge demanda ad un soggetto pubblico, le finalità:

(a) di gestione di asili nido;

(b) concernenti la gestione di mense scolastiche o la fornitura di sussidi, contributi e materiale didattico;

(c) ricreative o di promozione della cultura e dello sport, con particolare riferimento all'organizzazione di soggiorni, mostre, conferenze e manifestazioni sportive o all'uso di beni immobili o all'occupazione di suolo pubblico;

(d) di assegnazione di alloggi di edilizia residenziale pubblica;

(e) relative alla leva militare;

(f) di polizia amministrativa anche locale, salvo quanto previsto dall'articolo 53, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente, tutela delle risorse idriche e difesa del suolo;

(g) degli uffici per le relazioni con il pubblico;

(h) in materia di protezione civile;

(i) di supporto al collocamento e all'avviamento al lavoro, in particolare a cura di centri di iniziativa locale per l'occupazione e di sportelli-lavoro;

(j) dei difensori civici regionali e locali.

Capo V - Particolari contrassegni

Art. 74. Contrassegni su veicoli e accessi a centri storici

1. I contrassegni rilasciati a qualunque titolo per la circolazione e la sosta di veicoli a servizio di persone invalide, ovvero per il transito e la sosta in zone a traffico limitato, e che devono essere esposti su veicoli, contengono i soli dati indispensabili ad individuare l'autorizzazione rilasciata e senza l'apposizione di simboli o diciture dai quali può desumersi la speciale natura dell'autorizzazione per effetto della sola visione del contrassegno.

2. Le generalità e l'indirizzo della persona fisica interessata sono riportati sui contrassegni con modalità che non consentono, parimenti, la loro diretta visibilità se non in caso di richiesta di esibizione o necessità di accertamento.

3. La disposizione di cui al comma 2 si applica anche in caso di fissazione a qualunque titolo di un obbligo di esposizione sui veicoli di copia del libretto di circolazione o di altro documento.

4. Per il trattamento dei dati raccolti mediante impianti per la rilevazione degli accessi di veicoli ai centri storici ed alle zone a traffico limitato continuano, altresì, ad applicarsi le disposizioni del decreto del Presidente della Repubblica 22 giugno 1999, n. 250.

A.2.5 Titolo V - Trattamento di dati personali in ambito sanitario

Capo I - Principi generali

Art. 75. Ambito applicativo

1. Il presente titolo disciplina il trattamento dei dati personali in ambito sanitario.

Art. 76. Esercenti professioni sanitarie e organismi sanitari pubblici

1. Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi dell'articolo 85, trattano i dati personali idonei a rivelare lo stato di salute:

   (a) con il consenso dell'interessato e anche senza l'autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato;

   (b) anche senza il consenso dell'interessato e previa autorizzazione del Garante, se la finalità di cui alla lettera a) riguarda un terzo o la collettività.

2. Nei casi di cui al comma 1 il consenso può essere prestato con le modalità semplificate di cui al capo II.

3. Nei casi di cui al comma 1 l'autorizzazione del Garante è rilasciata, salvi i casi di particolare urgenza, sentito il Consiglio superiore di sanità.

Capo II - Modalità semplificate per informativa e consenso

Art. 77. Casi di semplificazione

1. Il presente capo individua modalità semplificate utilizzabili dai soggetti di cui al comma 2:
   (a) per informare l'interessato relativamente ai dati personali raccolti presso il medesimo interessato o presso terzi, ai sensi dell'articolo 13, commi 1 e 4;
   (b) per manifestare il consenso al trattamento dei dati personali nei casi in cui ciò è richiesto ai sensi dell'articolo 76;
   (c) per il trattamento dei dati personali.
2. Le modalità semplificate di cui al comma 1 sono applicabili:
   (a) dagli organismi sanitari pubblici;
   (b) dagli altri organismi privati e dagli esercenti le professioni sanitarie;
   (c) dagli altri soggetti pubblici indicati nell'articolo 80.

Art. 78. Informativa del medico di medicina generale o del pediatra

1. Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati nell'articolo 13, comma 1.
2. L'informativa può essere fornita per il complessivo trattamento dei dati personali necessario per attività di prevenzione, diagnosi, cura e riabilitazione, svolte dal medico o dal pediatra a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse.
3. L'informativa può riguardare, altresì, dati personali eventualmente raccolti presso terzi, ed è fornita preferibilmente per iscritto, anche attraverso carte tascabili con eventuali allegati pieghevoli, includendo almeno gli elementi indicati dal Garante ai sensi dell'articolo 13, comma 3, eventualmente integrati anche oralmente in relazione a particolari caratteristiche del trattamento.

4. L'informativa, se non è diversamente specificato dal medico o dal pediatra, riguarda anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che:

   (a) sostituisce temporaneamente il medico o il pediatra;

   (b) fornisce una prestazione specialistica su richiesta del medico e del pediatra;

   (c) può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata;

   (d) fornisce farmaci prescritti;

   (e) comunica dati personali al medico o pediatra in conformità alla disciplina applicabile.

5. L'informativa resa ai sensi del presente articolo evidenzia analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati:

   (a) per scopi scientifici, anche di ricerca scientifica e di sperimentazione clinica controllata di medicinali, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente;

   (b) nell'ambito della teleassistenza o telemedicina;

   (c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica.

Art. 79. Informativa da parte di organismi sanitari

1. Gli organismi sanitari pubblici e privati possono avvalersi delle modalità semplificate relative all'informativa e al consenso di cui agli articoli 78 e 81 in riferimento ad una pluralità di prestazioni erogate anche da distinti reparti ed unità dello stesso organismo o di più strutture ospedaliere o territoriali specificamente identificati.

2. Nei casi di cui al comma 1 l'organismo o le strutture annotano l'avvenuta informativa e il consenso con modalità uniformi e tali da permettere una verifica al riguardo da parte di altri reparti ed unità che, anche in tempi diversi, trattano dati relativi al medesimo interessato.

3. Le modalità semplificate di cui agli articoli 78 e 81 possono essere utilizzate in modo omogeneo e coordinato in riferimento all'insieme dei trattamenti di dati personali effettuati nel complesso delle strutture facenti capo alle aziende sanitarie.

4. Sulla base di adeguate misure organizzative in applicazione del comma 3, le modalità semplificate possono essere utilizzate per più trattamenti di dati effettuati nei casi di cui al presente articolo ed ai soggetti di cui all'articolo 80.

Art. 80. Informativa da parte di altri soggetti pubblici

1. Oltre a quanto previsto dall'articolo 79, possono avvalersi della facoltà di fornire un'unica informativa per una pluralità di trattamenti di dati effettuati, a fini amministrativi e in tempi diversi, rispetto a dati raccolti presso l'interessato e presso terzi, i competenti servizi o strutture di soggetti pubblici operanti in ambito sanitario o della prevenzione e sicurezza del lavoro.

2. L'informativa di cui al comma 1 è integrata con appositi e idonei cartelli ed avvisi agevolmente visibili al pubblico, affissi e diffusi anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica, in particolare per quanto riguarda attività amministrative di rilevante interesse pubblico che non richiedono il consenso degli interessati.

Art. 81. Prestazione del consenso

1. Il consenso al trattamento dei dati idonei a rivelare lo stato di salute, nei casi in cui è necessario ai sensi del presente codice o di altra disposizione di legge, può essere manifestato con un'unica dichiarazione, anche oralmente. In tal caso il consenso è documentato, anziché con atto scritto dell'interessato, con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico, riferita al trattamento di dati effettuato da uno o più soggetti e all'informativa all'interessato, nei modi indicati negli articoli 78, 79 e 80.

2. Quando il medico o il pediatra fornisce l'informativa per conto di più professionisti ai sensi dell'articolo 78, comma 4, oltre quanto previsto dal comma 1, il consenso è reso conoscibile ai medesimi professionisti con adeguate modalità, anche attraverso menzione, annotazione o

apposizione di un bollino o tagliando su una carta elettronica o sulla tessera sanitaria, contenente un richiamo al medesimo articolo 78, comma 4, e alle eventuali diverse specificazioni apposte all'informativa ai sensi del medesimo comma.

Art. 82. Emergenze e tutela della salute e dell'incolumità fisica

1. L'informativa e il consenso al trattamento dei dati personali possono intervenire senza ritardo, successivamente alla prestazione, nel caso di emergenza sanitaria o di igiene pubblica per la quale la competente autorità ha adottato un'ordinanza contingibile ed urgente ai sensi dell'articolo 117 del decreto legislativo 31 marzo 1998, n. 112.

2. L'informativa e il consenso al trattamento dei dati personali possono altresì intervenire senza ritardo, successivamente alla prestazione, in caso di:

   (a) impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato;

   (b) rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato.

3. L'informativa e il consenso al trattamento dei dati personali possono intervenire senza ritardo, successivamente alla prestazione, anche in caso di prestazione medica che può essere pregiudicata dall'acquisizione preventiva del consenso, in termini di tempestività o efficacia.

4. Dopo il raggiungimento della maggiore età l'informativa è fornita all'interessato anche ai fini della acquisizione di una nuova manifestazione del consenso quando questo è necessario.

Art. 83. Altre misure per il rispetto dei diritti degli interessati

1. I soggetti di cui agli articoli 78, 79 e 80 adottano idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalle leggi e dai regolamenti in materia di modalità di trattamento dei dati sensibili e di misure minime di sicurezza.

2. Le misure di cui al comma 1 comprendono, in particolare:

   (a) soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa all'interno di strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;

   (b) l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;

   (c) soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;

   (d) cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;

   (e) il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati;

   (f) la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso;

   (g) la formale previsione, in conformità agli ordinamenti interni delle strutture ospedaliere e territoriali, di adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, informandone previamente gli interessati e rispettando eventuali loro contrarie manifestazioni legittime di volontà;

   (h) la messa in atto di procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;

   (i) la sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.

2-bis. Le misure di cui al comma 2 non si applicano ai soggetti di cui all'articolo 78, che ottemperano alle disposizioni di cui al comma 1 secondo modalità adeguate a garantire un rapporto personale e fiduciario con gli assistiti, nel rispetto del codice di deontologia sottoscritto ai sensi dell'articolo 12.

Art. 84. Comunicazione di dati all'interessato

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 presente comma non si applica in riferimento ai dati personali forniti in precedenza dal medesimo interessato.

2. Il titolare o il responsabile possono autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a). L'atto di incarico individua appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati.

Capo III - Finalità di rilevante interesse pubblico

Art. 85. Compiti del Servizio sanitario nazionale

1. Fuori dei casi di cui al comma 2, si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità che rientrano nei compiti del Servizio sanitario nazionale e degli altri organismi sanitari pubblici relative alle seguenti attività:

   (a) attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal Servizio sanitario nazionale, ivi compresa l'assistenza degli stranieri in Italia e dei cittadini italiani all'estero, nonché di assistenza sanitaria erogata al personale navigante ed aeroportuale;

   (b) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;

   (c) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;

   (d) attività certificatorie;

   (e) l'applicazione della normativa in materia di igiene e sicurezza nei luoghi di lavoro e di sicurezza e salute della popolazione;

(f) le attività amministrative correlate ai trapianti d'organo e di tessuti, nonché alle trasfusioni di sangue umano, anche in applicazione della legge 4 maggio 1990, n. 107;

(g) instaurazione, gestione, pianificazione e controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati del Servizio sanitario nazionale.

2. Il comma 1 non si applica ai trattamenti di dati idonei a rivelare lo stato di salute effettuati da esercenti le professioni sanitarie o da organismi sanitari pubblici per finalità di tutela della salute o dell'incolumità fisica dell'interessato, di un terzo o della collettività, per i quali si osservano le disposizioni relative al consenso dell'interessato o all'autorizzazione del Garante ai sensi dell'articolo 76.

3. All'identificazione dei tipi di dati idonei a rivelare lo stato di salute e di operazioni su essi eseguibili è assicurata ampia pubblicità, anche tramite affissione di una copia o di una guida illustrativa presso ciascuna azienda sanitaria e presso gli studi dei medici di medicina generale e dei pediatri di libera scelta.

4. Il trattamento di dati identificativi dell'interessato è lecito da parte dei soli soggetti che perseguono direttamente le finalità di cui al comma 1. L'utilizzazione delle diverse tipologie di dati è consentita ai soli incaricati, preposti, caso per caso, alle specifiche fasi delle attività di cui al medesimo comma, secondo il principio dell'indispensabilità dei dati di volta in volta trattati.

Art. 86. Altre finalità di rilevante interesse pubblico

1. Fuori dei casi di cui agli articoli 76 e 85, si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità, perseguite mediante trattamento di dati sensibili e giudiziari, relative alle attività amministrative correlate all'applicazione della disciplina in materia di:

(a) tutela sociale della maternità e di interruzione volontaria della gravidanza, con particolare riferimento a quelle svolte per la gestione di consultori familiari e istituzioni analoghe, per l'informazione, la cura e la degenza delle madri, nonché per gli interventi di interruzione della gravidanza;

(b) stupefacenti e sostanze psicotrope, con particolare riferimento a quelle svolte al fine di assicurare, anche avvalendosi di enti ed associazioni senza fine di lucro, i servizi pubblici necessari per l'assistenza socio-sanitaria ai tossicodipendenti, gli interventi anche di tipo preventivo previsti dalle leggi e l'applicazione delle misure amministrative previste;

(c) assistenza, integrazione sociale e diritti delle persone handicappate effettuati, in particolare, al fine di:

i. accertare l'handicap ed assicurare la funzionalità dei servizi terapeutici e riabilitativi, di aiuto personale e familiare, nonché interventi economici integrativi ed altre agevolazioni;

ii. curare l'integrazione sociale, l'educazione, l'istruzione e l'informazione alla famiglia del portatore di handicap, nonché il collocamento obbligatorio nei casi previsti dalla legge;

iii. realizzare comunità-alloggio e centri socio riabilitativi;

iv. curare la tenuta degli albi degli enti e delle associazioni ed organizzazioni di volontariato impegnati nel settore.

2. Ai trattamenti di cui al presente articolo si applicano le disposizioni di cui all'articolo 85, comma 4.

Capo IV - Prescrizioni mediche

Art. 87. Medicinali a carico del Servizio sanitario nazionale

1. Le ricette relative a prescrizioni di medicinali a carico, anche parziale, del Servizio sanitario nazionale sono redatte secondo il modello di cui al comma 2, conformato in modo da permettere di risalire all'identità dell'interessato solo in caso di necessità connesse al controllo della correttezza della prescrizione, ovvero a fini di verifiche amministrative o per scopi epidemiologici e di ricerca, nel rispetto delle norme deontologiche applicabili.

2. Il modello cartaceo per le ricette di medicinali relative a prescrizioni di medicinali a carico, anche parziale, del Servizio sanitario nazionale, di cui agli allegati 1, 3, 5 e 6 del decreto del Ministro della sanità 11 luglio 1988, n. 350, e al capitolo 2, paragrafo 2.2.2. del relativo disciplinare tecnico, è integrato da un tagliando predisposto su carta o con tecnica di tipo copiativo e unito ai bordi delle zone indicate nel comma 3.

3. Il tagliando di cui al comma 2 è apposto sulle zone del modello predisposte per l'indicazione delle generalità e dell'indirizzo dell'assistito, in modo da consentirne la visione solo per effetto di una momentanea separazione del tagliando medesimo che risulti necessaria ai sensi dei commi 4 e 5.

4. Il tagliando può essere momentaneamente separato dal modello di ricetta, e successivamente riunito allo stesso, quando il farmacista lo ritiene indispensabile, mediante sottoscrizione apposta sul tagliando, per una effettiva necessità connessa al controllo della correttezza della prescrizione, anche per quanto riguarda la corretta fornitura del farmaco.

5. Il tagliando può essere momentaneamente separato nei modi di cui al comma 3 anche presso i competenti organi per fini di verifica amministrativa sulla correttezza della prescrizione, o da parte di soggetti legittimati a svolgere indagini epidemiologiche o di ricerca in conformità alla legge, quando è indispensabile per il perseguimento delle rispettive finalità.

6. Con decreto del Ministro della salute, sentito il Garante, può essere individuata una ulteriore soluzione tecnica diversa da quella indicata nel comma 1, basata sull'uso di una fascetta adesiva o su altra tecnica equipollente relativa anche a modelli non cartacei.

Art. 88. Medicinali non a carico del Servizio sanitario nazionale

1. Nelle prescrizioni cartacee di medicinali soggetti a prescrizione ripetibile non a carico, anche parziale, del Servizio sanitario nazionale, le generalità dell'interessato non sono indicate.

2. Nei casi di cui al comma 1 il medico può indicare le generalità dell'interessato solo se ritiene indispensabile permettere di risalire alla sua identità, per un'effettiva necessità derivante dalle particolari condizioni del medesimo interessato o da una speciale modalità di preparazione o di utilizzazione.

Art. 89. Casi particolari

1. Le disposizioni del presente capo non precludono l'applicazione di disposizioni normative che prevedono il rilascio di ricette che non identificano l'interessato o recanti particolari annotazioni, contenute anche nel decreto-legge 17 febbraio 1998, n. 23, convertito, con modificazioni, dalla legge 8 aprile 1998, n. 94.

2. Nei casi in cui deve essere accertata l'identità dell'interessato ai sensi del testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e successive modificazioni, le ricette sono conservate separatamente da ogni altro documento che non ne richiede l'utilizzo.

3.

2-bis. Per i soggetti di cui all'articolo 78, l'attuazione delle disposizioni di cui all'articolo 87, comma 3, e 88, comma 1, è subordinata ad un'esplicita richiesta dell'interessato.

Capo V - Dati genetici

Art. 90. Trattamento dei dati genetici e donatori di midollo osseo

1. Il trattamento dei dati genetici da chiunque effettuato è consentito nei soli casi previsti da apposita autorizzazione rilasciata dal Garante sentito il Ministro della salute, che acquisisce, a tal fine, il parere del Consiglio superiore di sanità.

2. L'autorizzazione di cui al comma 1 individua anche gli ulteriori elementi da includere nell'informativa ai sensi dell'articolo 13, con particolare riguardo alla specificazione delle finalità perseguite e dei risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati e al diritto di opporsi al medesimo trattamento per motivi legittimi.

3. Il donatore di midollo osseo, ai sensi della legge 6 marzo 2001, n. 52, ha il diritto e il dovere di mantenere l'anonimato sia nei confronti del ricevente sia nei confronti di terzi.

Capo VI - Disposizioni varie

Art. 91. Dati trattati mediante carte

1. Il trattamento in ogni forma di dati idonei a rivelare lo stato di salute o la vita sessuale eventualmente registrati su carte anche non elettroniche, compresa la carta nazionale dei servizi, o trattati mediante le medesime carte è consentito se necessario ai sensi dell'articolo 3, nell'osservanza di misure ed accorgimenti prescritti dal Garante nei modi di cui all'articolo 17.

Art. 92. Cartelle cliniche

1. Nei casi in cui organismi sanitari pubblici e privati redigono e conservano una cartella clinica in conformità alla disciplina applicabile, sono adottati opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri.

2. Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

   (a) di far valere o difendere un diritto in sede giudiziaria ai sensi dell'articolo 26, comma 4, lettera c), di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

   (b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Art. 93. Certificato di assistenza al parto

1. Ai fini della dichiarazione di nascita il certificato di assistenza al parto è sempre sostituito da una semplice attestazione contenente i soli dati richiesti nei registri di nascita. Si osservano, altresì, le disposizioni dell'articolo 109.

2. Il certificato di assistenza al parto o la cartella clinica, ove comprensivi dei dati personali che rendono identificabile la madre che abbia dichiarato di non voler essere nominata avvalendosi della facoltà di cui all'articolo 30, comma 1, del decreto del Presidente della Repubblica 3 novembre 2000, n. 396, possono essere rilasciati in copia integrale a chi vi abbia interesse, in conformità alla legge, decorsi cento anni dalla formazione del documento.

3. Durante il periodo di cui al comma 2 la richiesta di accesso al certificato o alla cartella può essere accolta relativamente ai dati relativi alla

madre che abbia dichiarato di non voler essere nominata, osservando le opportune cautele per evitare che quest'ultima sia identificabile.

Art. 94. Banche di dati, registri e schedari in ambito sanitario

1. Il trattamento di dati idonei a rivelare lo stato di salute contenuti in banche di dati, schedari, archivi o registri tenuti in ambito sanitario, è effettuato nel rispetto dell'articolo 3 anche presso banche di dati, schedari, archivi o registri già istituiti alla data di entrata in vigore del presente codice e in riferimento ad accessi di terzi previsti dalla disciplina vigente alla medesima data, in particolare presso:

   (a) il registro nazionale dei casi di mesotelioma asbesto-correlati istituito presso l'Istituto superiore per la prevenzione e la sicurezza del lavoro (Ispesl), di cui all'articolo 1 del decreto del Presidente del Consiglio dei ministri 10 dicembre 2002, n. 308;

   (b) la banca di dati in materia di sorveglianza della malattia di Creutzfeldt-Jakob o delle varianti e sindromi ad essa correlate, di cui al decreto del Ministro della salute in data 21 dicembre 2001, pubblicato nella Gazzetta Ufficiale n. 8 del 10 gennaio 2002;

   (c) il registro nazionale delle malattie rare di cui all'articolo 3 del decreto del Ministro della sanità in data 18 maggio 2001, n. 279;

   (d) i registri dei donatori di midollo osseo istituiti in applicazione della legge 6 marzo 2001, n. 52;

   (e) gli schedari dei donatori di sangue di cui all'articolo 15 del decreto del Ministro della sanità in data 26 gennaio 2001, pubblicato nella Gazzetta Ufficiale n. 78 del 3 aprile 2001.

A.2.6 Titolo VI - Istruzione

Capo I - Profili generali

Art. 95. Dati sensibili e giudiziari

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di istruzione e di formazione in ambito scolastico, professionale, superiore o universitario, con particolare riferimento a quelle svolte anche in forma integrata.

Art. 96. Trattamento di dati relativi a studenti

1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le scuole e gli istituti scolastici di istruzione secondaria, su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle predette finalità e indicati nell'informativa resa agli interessati ai sensi dell'articolo 13. I dati possono essere successivamente trattati esclusivamente per le predette finalità.

2. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.

A.2.7 Titolo VII - Trattamento per scopi storici, statistici o scientifici

Capo I - Profili generali

Art. 97. Ambito applicativo

1. Il presente titolo disciplina il trattamento dei dati personali effettuato per scopi storici, statistici o scientifici.

Art. 98. Finalità di rilevante interesse pubblico

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità relative ai trattamenti effettuati da soggetti pubblici:

   (a) per scopi storici, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato e negli archivi storici degli enti pubblici, secondo quanto disposto dal decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali, come modificato dal presente codice;

(b) che fanno parte del Sistema statistico nazionale (Sistan) ai sensi del decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni;

(c) per scopi scientifici.

Art. 99. Compatibilità tra scopi e durata del trattamento

1. Il trattamento di dati personali effettuato per scopi storici, statistici o scientifici è considerato compatibile con i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

2. Il trattamento di dati personali per scopi storici, statistici o scientifici può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

3. Per scopi storici, statistici o scientifici possono comunque essere conservati o ceduti ad altro titolare i dati personali dei quali, per qualsiasi causa, è cessato il trattamento.

Art. 100. Dati relativi ad attività di studio e ricerca

1. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico i soggetti pubblici, ivi comprese le università e gli enti di ricerca, possono con autonome determinazioni comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione di quelli sensibili o giudiziari.

2. Resta fermo il diritto dell'interessato di opporsi per motivi legittimi ai sensi dell'articolo 7, comma 4, lettera a).

3. I dati di cui al presente articolo non costituiscono documenti amministrativi ai sensi della legge 7 agosto 1990, n. 241.

4. I dati di cui al presente articolo possono essere successivamente trattati per i soli scopi in base ai quali sono comunicati o diffusi.

Capo II - Trattamento per scopi storici

Art. 101. Modalità di trattamento

1. I dati personali raccolti per scopi storici non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità nel rispetto dell'articolo 11.

2. I documenti contenenti dati personali, trattati per scopi storici, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi. I dati personali diffusi possono essere utilizzati solo per il perseguimento dei medesimi scopi.

3. I dati personali possono essere comunque diffusi quando sono relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso suoi comportamenti in pubblico.

Art. 102. Codice di deontologia e di buona condotta

1. Il Garante promuove ai sensi dell'articolo 12 la sottoscrizione di un codice di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi storici.

2. Il codice di deontologia e di buona condotta di cui al comma 1 individua, in particolare:

   (a) le regole di correttezza e di non discriminazione nei confronti degli utenti da osservare anche nella comunicazione e diffusione dei dati, in armonia con le disposizioni del presente codice applicabili ai trattamenti di dati per finalità giornalistiche o di pubblicazione di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica;

   (b) le particolari cautele per la raccolta, la consultazione e la diffusione di documenti concernenti dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare, identificando casi in cui l'interessato o chi vi abbia interesse è informato dall'utente della prevista diffusione di dati;

   (c) le modalità di applicazione agli archivi privati della disciplina dettata in materia di trattamento dei dati a scopi storici, anche in riferimento all'uniformità dei criteri da seguire per la consultazione e alle cautele da osservare nella comunicazione e nella diffusione.

Art. 103. Consultazione di documenti conservati in archivi

1. La consultazione dei documenti conservati negli archivi di Stato, in quelli storici degli enti pubblici e in archivi privati è disciplinata dal decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali, come modificato dal presente codice.

Capo III - Trattamento per scopi statistici o scientifici

Art. 104. Ambito applicativo e dati identificativi per scopi statistici o scientifici

1. Le disposizioni del presente capo si applicano ai trattamenti di dati per scopi statistici o, in quanto compatibili, per scopi scientifici.

2. Agli effetti dell'applicazione del presente capo, in relazione ai dati identificativi si tiene conto dell'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare o da altri per identificare l'interessato, anche in base alle conoscenze acquisite in relazione al progresso tecnico.

Art. 105. Modalità di trattamento

1. I dati personali trattati per scopi statistici o scientifici non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti di dati per scopi di altra natura.

2. Gli scopi statistici o scientifici devono essere chiaramente determinati e resi noti all'interessato, nei modi di cui all'articolo 13 anche in relazione a quanto previsto dall'articolo 106, comma 2, lettera b), del presente codice e dall'articolo 6-bis del decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni.

3. Quando specifiche circostanze individuate dai codici di cui all'articolo 106 sono tali da consentire ad un soggetto di rispondere in nome e per conto di un altro, in quanto familiare o convivente, l'informativa all'interessato può essere data anche per il tramite del soggetto rispondente.

4. Per il trattamento effettuato per scopi statistici o scientifici rispetto a dati raccolti per altri scopi, l'informativa all'interessato non è dovuta quando richiede uno sforzo sproporzionato rispetto al diritto tutelato, se sono adottate le idonee forme di pubblicità individuate dai codici di cui all'articolo 106.

Art. 106. Codici di deontologia e di buona condotta

1. Il Garante promuove ai sensi dell'articolo 12 la sottoscrizione di uno o più codici di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi statistici o scientifici.

2. Con i codici di cui al comma 1 sono individuati, tenendo conto, per i soggetti già compresi nell'ambito del Sistema statistico nazionale, di quanto già previsto dal decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni, e, per altri soggetti, sulla base di analoghe garanzie, in particolare:

   (a) i presupposti e i procedimenti per documentare e verificare che i trattamenti, fuori dai casi previsti dal medesimo decreto legislativo n. 322 del 1989, siano effettuati per idonei ed effettivi scopi statistici o scientifici;

   (b) per quanto non previsto dal presente codice, gli ulteriori presupposti del trattamento e le connesse garanzie, anche in riferimento alla durata della conservazione dei dati, alle informazioni da rendere agli interessati relativamente ai dati raccolti anche presso terzi, alla comunicazione e diffusione, ai criteri selettivi da osservare per il trattamento di dati identificativi, alle specifiche misure di sicurezza e alle modalità per la modifica dei dati a seguito dell'esercizio dei diritti dell'interessato, tenendo conto dei principi contenuti nelle pertinenti raccomandazioni del Consiglio d'Europa;

   (c) l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare del trattamento o da altri per identificare l'interessato, anche in relazione alle conoscenze acquisite in base al progresso tecnico;

   (d) le garanzie da osservare ai fini dell'applicazione delle disposizioni di cui all'articolo 24, comma 1, lettera i), e 43, comma 1, lettera g), che permettono di prescindere dal consenso dell'interessato, tenendo conto dei principi contenuti nelle predette raccomandazioni;

   (e) modalità semplificate per la prestazione del consenso degli interessati relativamente al trattamento dei dati sensibili;

   (f) le regole di correttezza da osservare nella raccolta dei dati e le istruzioni da impartire al personale incaricato;

(g) le misure da adottare per favorire il rispetto dei principi di pertinenza e non eccedenza dei dati e delle misure di sicurezza di cui all'articolo 31, anche in riferimento alle cautele volte ad impedire l'accesso da parte di persone fisiche che non sono incaricati e l'identificazione non autorizzata degli interessati, all'interconnessione dei sistemi informativi anche nell'ambito del Sistema statistico nazionale e all'interscambio di dati per scopi statistici o scientifici da effettuarsi con enti ed uffici situati all'estero anche sulla base delle garanzie previste dall'articolo 44, comma 1, lettera a);

(h) l'impegno al rispetto di regole di condotta degli incaricati che non sono tenuti in base alla legge al segreto d'ufficio o professionale, tali da assicurare analoghi livelli di sicurezza e di riservatezza.

Art. 107. Trattamento di dati sensibili

1. Fermo restando quanto previsto dall'articolo 20 e fuori dei casi di particolari indagini statistiche o di ricerca scientifica previste dalla legge, il consenso dell'interessato al trattamento di dati sensibili, quando è richiesto, può essere prestato con modalità semplificate, individuate dal codice di cui all'articolo 106 e l'autorizzazione del Garante può essere rilasciata anche ai sensi dell'articolo 40.

Art. 108. Sistema statistico nazionale

1. Il trattamento di dati personali da parte di soggetti che fanno parte del Sistema statistico nazionale, oltre a quanto previsto dal codice di deontologia e di buona condotta sottoscritto ai sensi dell'articolo 106, comma 2, resta inoltre disciplinato dal decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni, in particolare per quanto riguarda il trattamento dei dati sensibili indicati nel programma statistico nazionale, l'informativa all'interessato, l'esercizio dei relativi diritti e i dati non tutelati dal segreto statistico ai sensi dell'articolo 9, comma 4, del medesimo decreto.

Art. 109. Dati statistici relativi all'evento della nascita

1. Per la rilevazione dei dati statistici relativi agli eventi di nascita, compresi quelli relativi ai nati affetti da malformazioni e ai nati morti,

nonché per i flussi di dati anche da parte di direttori sanitari, si osservano, oltre alle disposizioni di cui al decreto del Ministro della sanità 16 luglio 2001, n. 349, le modalità tecniche determinate dall'Istituto nazionale della statistica, sentito il Ministro della salute, dell'interno e il Garante.

Art. 110. Ricerca medica, biomedica ed epidemiologica

1. Il consenso dell'interessato per il trattamento dei dati idonei a rivelare lo stato di salute, finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è prevista da un'espressa disposizione di legge che prevede specificamente il trattamento, ovvero rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, e successive modificazioni, e per il quale sono decorsi quarantacinque giorni dalla comunicazione al Garante ai sensi dell'articolo 39. Il consenso non è inoltre necessario quando a causa di particolari ragioni non è possibile informare gli interessati e il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale ed è autorizzato dal Garante anche ai sensi dell'articolo 40.

2. In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 7 nei riguardi dei trattamenti di cui al comma 1, l'aggiornamento, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.

A.2.8 Titolo VIII - Lavoro e previdenza sociale

Capo I - Profili generali

Art. 111. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato per finalità previdenziali o per la gestione del rapporto di lavoro, prevedendo anche specifiche modalità per l'informativa all'interessato e per l'eventuale prestazione del consenso relativamente alla pubblicazione degli annunci per finalità di occupazione di cui all'articolo 113, comma 3 e alla ricezione di curricula contenenti dati personali anche sensibili.

Art. 112. Finalità di rilevante interesse pubblico

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di instaurazione e gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato.

2. Tra i trattamenti effettuati per le finalità di cui al comma 1, si intendono ricompresi, in particolare, quelli effettuati al fine di:

   (a) applicare la normativa in materia di collocamento obbligatorio e assumere personale anche appartenente a categorie protette;

   (b) garantire le pari opportunità;

   (c) accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, anche in materia di tutela delle minoranze linguistiche, ovvero la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, il trasferimento di sede per incompatibilità e il conferimento di speciali abilitazioni;

   (d) adempiere ad obblighi connessi alla definizione dello stato giuridico ed economico, ivi compreso il riconoscimento della causa di servizio o dell'equo indennizzo, nonché ad obblighi retributivi, fiscali o contabili, relativamente al personale in servizio o in quiescenza, ivi compresa la corresponsione di premi e benefici assistenziali;

   (e) adempiere a specifici obblighi o svolgere compiti previsti dalla normativa in materia di igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, nonché in materia sindacale;

   (f) applicare, anche da parte di enti previdenziali ed assistenziali, la normativa in materia di previdenza ed assistenza ivi compresa quella integrativa, anche in applicazione del decreto legislativo del Capo provvisorio dello Stato 29 luglio 1947, n. 804, riguardo alla comunicazione di dati, anche mediante reti di comunicazione elettronica, agli istituti di patronato e di assistenza sociale, alle associazioni di categoria e agli ordini professionali che abbiano ottenuto il consenso dell'interessato ai sensi dell'articolo 23 in relazione a tipi di dati individuati specificamente;

   (g) svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile ed esaminare i ricorsi amministrativi in conformità alle norme che regolano le rispettive materie;

(h) comparire in giudizio a mezzo di propri rappresentanti o partecipare alle procedure di arbitrato o di conciliazione nei casi previsti dalla legge o dai contratti collettivi di lavoro;

(i) salvaguardare la vita o l'incolumità fisica dell'interessato o di terzi;

(j) gestire l'anagrafe dei pubblici dipendenti e applicare la normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti;

(k) applicare la normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale;

(l) svolgere l'attività di indagine e ispezione presso soggetti pubblici;

(m) valutare la qualità dei servizi resi e dei risultati conseguiti.

3. La diffusione dei dati di cui alle lettere m), n) ed o) del comma 2 è consentita in forma anonima e, comunque, tale da non consentire l'individuazione dell'interessato.

Capo II - Annunci di lavoro e dati riguardanti prestatori di lavoro

Art. 113. Raccolta di dati e pertinenza

1. Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n. 300.

Capo III - Divieto di controllo a distanza e telelavoro

Art. 114. Controllo a distanza

1. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300.

Art. 115. Telelavoro e lavoro a domicilio

1. Nell'ambito del rapporto di lavoro domestico e del telelavoro il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale.

2. Il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare.

Capo IV - Istituti di patronato e di assistenza sociale

Art. 116. Conoscibilità di dati su mandato dell'interessato

1. Per lo svolgimento delle proprie attività gli istituti di patronato e di assistenza sociale, nell'ambito del mandato conferito dall'interessato, possono accedere alle banche di dati degli enti eroganti le prestazioni, in relazione a tipi di dati individuati specificamente con il consenso manifestato ai sensi dell'articolo 23.

2. Il Ministro del lavoro e delle politiche sociali stabilisce con proprio decreto le linee-guida di apposite convenzioni da stipulare tra gli istituti di patronato e di assistenza sociale e gli enti eroganti le prestazioni.

A.2.9 Titolo IX - Sistema bancario, finanziario ed assicurativo

Capo I - Sistemi informativi

Art. 117. Affidabilità e puntualità nei pagamenti

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di concessione di crediti al consumo o comunque riguardanti l'affidabilità e la puntualità nei pagamenti da parte degli interessati, individuando anche specifiche modalità per garantire la comunicazione di dati personali esatti e aggiornati nel rispetto dei diritti dell'interessato.

Art. 118. Informazioni commerciali

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale, prevedendo anche, in correlazione con quanto previsto dall' articolo 13, comma 5, modalità semplificate per l'informativa all'interessato e idonei meccanismi per garantire la qualità e l'esattezza dei dati raccolti e comunicati.

Art. 119. Dati relativi al comportamento debitorio

1. Con il codice di deontologia e di buona condotta di cui all'articolo 118 sono altresì individuati termini armonizzati di conservazione dei dati personali contenuti, in particolare, in banche di dati, registri ed elenchi tenuti da soggetti pubblici e privati, riferiti al comportamento debitorio dell'interessato nei casi diversi da quelli disciplinati nel codice di cui all'articolo 117, tenendo conto della specificità dei trattamenti nei diversi ambiti.

Art. 120. Sinistri

1. L'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo (ISVAP) definisce con proprio provvedimento le procedure e le modalità di funzionamento della banca di dati dei sinistri istituita per la prevenzione e il contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie per i veicoli a motore immatricolati in Italia, stabilisce le modalità di accesso alle informazioni raccolte dalla banca dati per gli organi giudiziari e per le pubbliche amministrazioni competenti in materia di prevenzione e contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie, nonché le modalità e i limiti per l'accesso alle informazioni da parte delle imprese di assicurazione.

2. Il trattamento e la comunicazione ai soggetti di cui al comma 1 dei dati personali sono consentiti per lo svolgimento delle funzioni indicate nel medesimo comma.

3. Per quanto non previsto dal presente articolo si applicano le disposizioni dell'articolo 135 del Codice delle assicurazioni private.

A.2.10 Titolo X - Comunicazioni elettroniche

Capo I - Servizi di comunicazione elettronica

Art. 121. Servizi interessati

1. Le disposizioni del presente titolo si applicano al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni.

Art. 122. Informazioni raccolte nei riguardi dell'abbonato o dell'utente

1. Salvo quanto previsto dal comma 2, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente.

2. Il codice di deontologia di cui all'articolo 133 individua i presupposti e i limiti entro i quali l'uso della rete nei modi di cui al comma 1, per determinati scopi legittimi relativi alla memorizzazione tecnica per il tempo strettamente necessario alla trasmissione della comunicazione o a fornire uno specifico servizio richiesto dall'abbonato o dall'utente, è consentito al fornitore del servizio di comunicazione elettronica nei riguardi dell'abbonato e dell'utente che abbiano espresso il consenso sulla base di una previa informativa ai sensi dell'articolo 13 che indichi analiticamente, in modo chiaro e preciso, le finalità e la durata del trattamento.

Art. 123. Dati relativi al traffico

1. I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5.

2. Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se l'abbonato o l'utente cui i dati si riferiscono hanno manifestato il proprio consenso, che è revocabile in ogni momento.

4. Nel fornire l'informativa di cui all'articolo 13 il fornitore del servizio informa l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3.

5. Il trattamento dei dati personali relativi al traffico è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30 sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per lo svolgimento di tali attività e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

6. L'Autorità per le garanzie nelle comunicazioni può ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione di controversie attinenti, in particolare, all'interconnessione o alla fatturazione.

Art. 124. Fatturazione dettagliata

1. L'abbonato ha diritto di ricevere in dettaglio, a richiesta e senza alcun aggravio di spesa, la dimostrazione degli elementi che compongono la fattura relativi, in particolare, alla data e all'ora di inizio della conversazione, al numero selezionato, al tipo di numerazione, alla località, alla durata e al numero di scatti addebitati per ciascuna conversazione.

2. Il fornitore del servizio di comunicazione elettronica accessibile al pubblico è tenuto ad abilitare l'utente ad effettuare comunicazioni e a richiedere servizi da qualsiasi terminale, gratuitamente ed in modo agevole, avvalendosi per il pagamento di modalità alternative alla fatturazione, anche impersonali, quali carte di credito o di debito o carte prepagate.

3. Nella documentazione inviata all'abbonato relativa alle comunicazioni effettuate non sono evidenziati i servizi e le comunicazioni di cui al comma 2, né le comunicazioni necessarie per attivare le modalità alternative alla fatturazione.

4. Nella fatturazione all'abbonato non sono evidenziate le ultime tre cifre dei numeri chiamati. Ad esclusivi fini di specifica contestazione dell'esattezza di addebiti determinati o riferiti a periodi limitati, l'abbonato può richiedere la comunicazione dei numeri completi delle comunicazioni in questione.

5. Il Garante, accertata l'effettiva disponibilità delle modalità di cui al comma 2, può autorizzare il fornitore ad indicare nella fatturazione i numeri completi delle comunicazioni.

Art. 125. Identificazione della linea

1. Se è disponibile la presentazione dell'identificazione della linea chiamante, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'utente chiamante la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea chiamante, chiamata per chiamata. L'abbonato chiamante deve avere tale possibilità linea per linea.

2. Se è disponibile la presentazione dell'identificazione della linea chiamante, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'abbonato chiamato la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione delle chiamate entranti.

3. Se è disponibile la presentazione dell'identificazione della linea chiamante e tale indicazione avviene prima che la comunicazione sia stabilita, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'abbonato chiamato la possibilità, mediante una funzione semplice e gratuita, di respingere le chiamate entranti se la presentazione dell'identificazione della linea chiamante è stata eliminata dall'utente o abbonato chiamante.

4. Se è disponibile la presentazione dell'identificazione della linea collegata, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'abbonato chiamato la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea collegata all'utente chiamante.

5. Le disposizioni di cui al comma 1 si applicano anche alle chiamate dirette verso Paesi non appartenenti all'Unione europea. Le disposizioni di cui ai commi 2, 3 e 4 si applicano anche alle chiamate provenienti da tali Paesi.

6. Se è disponibile la presentazione dell'identificazione della linea chiamante o di quella collegata, il fornitore del servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e gli utenti dell'esistenza di tale servizio e delle possibilità previste ai commi 1, 2, 3 e 4.

Art. 126. Dati relativi all'ubicazione

1. I dati relativi all'ubicazione diversi dai dati relativi al traffico, riferiti agli utenti o agli abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, possono essere trattati solo se anonimi o se l'utente o l'abbonato ha manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto.

2. Il fornitore del servizio, prima di richiedere il consenso, informa gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti al trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto.

3. L'utente e l'abbonato che manifestano il proprio consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, conservano il diritto di richiedere, gratuitamente e mediante una funzione semplice, l'interruzione temporanea del trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni.

4. Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico, ai sensi dei commi 1, 2 e 3, è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30, sono la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni o del terzo che fornisce il servizio a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per la fornitura del servizio a valore aggiunto e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

Art. 127. Chiamate di disturbo e di emergenza

1. L'abbonato che riceve chiamate di disturbo può richiedere che il fornitore della rete pubblica di comunicazioni o del servizio di comunicazione elettronica accessibile al pubblico renda temporaneamente inefficace

la soppressione della presentazione dell'identificazione della linea chiamante e conservi i dati relativi alla provenienza della chiamata ricevuta. L'inefficacia della soppressione può essere disposta per i soli orari durante i quali si verificano le chiamate di disturbo e per un periodo non superiore a quindici giorni.

2. La richiesta formulata per iscritto dall'abbonato specifica le modalità di ricezione delle chiamate di disturbo e nel caso in cui sia preceduta da una richiesta telefonica è inoltrata entro quarantotto ore.

3. I dati conservati ai sensi del comma 1 possono essere comunicati all'abbonato che dichiari di utilizzarli per esclusive finalità di tutela rispetto a chiamate di disturbo. Per i servizi di cui al comma 1 il fornitore assicura procedure trasparenti nei confronti degli abbonati e può richiedere un contributo spese non superiore ai costi effettivamente sopportati.

4. Il fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico predispone procedure trasparenti per garantire, linea per linea, l'inefficacia della soppressione dell'identificazione della linea chiamante, nonché, ove necessario, il trattamento dei dati relativi all'ubicazione, nonostante il rifiuto o il mancato consenso temporanei dell'abbonato o dell'utente, da parte dei servizi abilitati in base alla legge a ricevere chiamate d'emergenza. I servizi sono individuati con decreto del Ministro delle comunicazioni, sentiti il Garante e l'Autorità per le garanzie nelle comunicazioni.

Art. 128. Trasferimento automatico della chiamata

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta le misure necessarie per consentire a ciascun abbonato, gratuitamente e mediante una funzione semplice, di poter bloccare il trasferimento automatico delle chiamate verso il proprio terminale effettuato da terzi.

Art. 129. Elenchi di abbonati(1)

1. Il Garante individua con proprio provvedimento, in cooperazione con l'Autorità per le garanzie nelle comunicazioni ai sensi dell'articolo 154, comma 3, e in conformità alla normativa comunitaria, le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi cartacei o elettronici a disposizione del pubblico,

anche in riferimento ai dati già raccolti prima della data di entrata in vigore del presente codice.

2. Il provvedimento di cui al comma 1 individua idonee modalità per la manifestazione del consenso all'inclusione negli elenchi e, rispettivamente, all'utilizzo dei dati per le finalità di cui all'articolo 7, comma 4, lettera b), in base al principio della massima semplificazione delle modalità di inclusione negli elenchi a fini di mera ricerca dell'abbonato per comunicazioni interpersonali, e del consenso specifico ed espresso qualora il trattamento esuli da tali fini, nonché in tema di verifica, rettifica o cancellazione dei dati senza oneri.

(1) La legge 27 febbraio 2009, n. 14, in sede di conversione con modificazioni del decreto-legge 30 dicembre 2008, n. 207, vi ha aggiunto il seguente comma: ***Art. 44 - Disposizioni in materia di tutela della riservatezza*** *[...]*
1-bis - I dati personali presenti nelle banche dati costituite sulla base di elenchi telefonici formati prima del 1° agosto 2005 sono lecitamente utilizzabili per fini promozionali sino al 31 dicembre 2009, anche in deroga agli articoli 13 e 23 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, dai soli titolari del trattamento che hanno provveduto a costituire dette banche dati prima del 1° agosto 2005. [...]

Art. 130. Comunicazioni indesiderate

1. L'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato

2. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo.

3. Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 23 e 24 nonchè ai sensi di quanto previsto dal comma 3-bis del presente articolo (1).

   3-bis. (2) In deroga a quanto previsto dall'articolo 129, il trattamento dei dati di cui all'articolo 129, comma 1, mediante l'impiego del telefono per le finalità di cui all'articolo 7, comma 4, lettera b), è consentito

nei confronti di chi non abbia esercitato il diritto di opposizione, con modalità semplificate e anche in via telematica, mediante l'iscrizione della numerazione della quale è intestatario in un registro pubblico delle opposizioni.

3-ter. (2) Il registro di cui al comma 3-bis è istituito con decreto del Presidente della Repubblica da adottare ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, previa deliberazione del Consiglio dei ministri, acquisito il parere del Consiglio di Stato e delle Commissioni parlamentari competenti in materia, che si pronunciano entro trenta giorni dalla richiesta, nonché, per i relativi profili di competenza, il parere dell'Autorità per le garanzie nelle comunicazioni, che si esprime entro il medesimo termine, secondo i seguenti criteri e princìpi generali:

(a) attribuzione dell'istituzione e della gestione del registro ad un ente o organismo pubblico titolare di competenze inerenti alla materia;

(b) previsione che l'ente o organismo deputato all'istituzione e alla gestione del registro vi provveda con le risorse umane e strumentali di cui dispone o affidandone la realizzazione e la gestione a terzi, che se ne assumono interamente gli oneri finanziari e organizzativi, mediante contratto di servizio, nel rispetto del codice dei contratti pubblici relativi a lavori, servizi e forniture, di cui al decreto legislativo 12 aprile 2006, n. 163. I soggetti che si avvalgono del registro per effettuare le comunicazioni corrispondono tariffe di accesso basate sugli effettivi costi di funzionamento e di manutenzione. Il Ministro dello sviluppo economico, con proprio provvedimento, determina tali tariffe;

(c) previsione che le modalità tecniche di funzionamento del registro consentano ad ogni utente di chiedere che sia iscritta la numerazione della quale è intestatario secondo modalità semplificate ed anche in via telematica o telefonica;

(d) previsione di modalità tecniche di funzionamento e di accesso al registro mediante interrogazioni selettive che non consentano il trasferimento dei dati presenti nel registro stesso, prevedendo il tracciamento delle operazioni compiute e la conservazione dei dati relativi agli accessi;

(e) disciplina delle tempistiche e delle modalità dell'iscrizione al registro, senza distinzione di settore di attività o di categoria merceologica, e del relativo aggiornamento, nonché del correlativo periodo

massimo di utilizzabilità dei dati verificati nel registro medesimo, prevedendosi che l'iscrizione abbia durata indefinita e sia revocabile in qualunque momento, mediante strumenti di facile utilizzo e gratuitamente;

(f) obbligo per i soggetti che effettuano trattamenti di dati per le finalità di cui all'articolo 7, comma 4, lettera b), di garantire la presentazione dell'identificazione della linea chiamante e di fornire all'utente idonee informative, in particolare sulla possibilità e sulle modalità di iscrizione nel registro per opporsi a futuri contatti;

(g) previsione che l'iscrizione nel registro non precluda i trattamenti dei dati altrimenti acquisiti e trattati nel rispetto degli articoli 23 e 24.

3-quater. (2) La vigilanza e il controllo sull'organizzazione e il funzionamento del registro di cui al comma 3-bis e sul trattamento dei dati sono attribuiti al Garante

4. Fatto salvo quanto previsto nel comma 1, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.

5. É vietato in ogni caso l'invio di comunicazioni per le finalità di cui al comma 1 o, comunque, a scopo promozionale, effettuato camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'articolo 7.

6. In caso di reiterata violazione delle disposizioni di cui al presente articolo il Garante può, provvedendo ai sensi dell'articolo 143, comma 1, lettera b), altresì prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni.

(1) Comma così modificato dalla lettera a) del comma 1 dell'art. 20-bis, D.L. 25 settembre 2009, n. 135, aggiunto dalla relativa legge di conversione 20 novembre 2009, n. 166.
(2) Comma aggiunto dalla lettera b) del comma 1 dell'art. 20-bis, D.L. 25 settembre 2009, n. 135, nel testo integrato dalla relativa legge di conversione 20 novembre 2009, n. 166.
Al fine di delineare con completezza il quadro normativo vigente in materia, si riportano i commi 2, 3 e 4 dell'art. 20-bis della legge 20 novembre 2009, n. 166 di conversione, con modificazioni, del D.L. 25 settembre 2009, n. 135.

2. Il registro previsto dall' articolo 130, comma 3-bis, del codice di cui al decreto legislativo 30 giugno 2003, n. 196, introdotto dal comma 1, lettera b), del presente articolo, è istituito entro sei mesi dalla data di entrata in vigore della legge di conversione del presente decreto. Fino al suddetto termine, restano in vigore i provvedimenti adottati dal Garante per la protezione dei dati personali ai sensi dell' articolo 154 del citato codice di cui al decreto legislativo n. 196 del 2003, e successive modificazioni, in attuazione dell' articolo 129 del medesimo codice.
3. All' articolo 44, comma 1-bis, del decreto-legge 30 dicembre 2008, n. 207, convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14, le parole: sino al 31 dicembre 2009 sono sostituite dalle seguenti: sino al termine di sei mesi successivi alla data di entrata in vigore della legge di conversione del decreto-legge 25 settembre 2009, n. 135.
4. All' articolo 58 del codice del consumo, di cui al decreto legislativo 6 settembre 2005, n. 206, il comma 1 è sostituito dal seguente:
1. L'impiego da parte di un professionista del telefono, della posta elettronica, di sistemi automatizzati di chiamata senza l'intervento di un operatore o di fax richiede il consenso preventivo del consumatore, fatta salva la disciplina prevista dall' articolo 130, comma 3-bis, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, per i trattamenti dei dati inclusi negli elenchi di abbonati a disposizione del pubblico.

Art. 131. Informazioni ad abbonati e utenti

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa l'abbonato e, ove possibile, l'utente circa la sussistenza di situazioni che permettono di apprendere in modo non intenzionale il contenuto di comunicazioni o conversazioni da parte di soggetti ad esse estranei.

2. L'abbonato informa l'utente quando il contenuto delle comunicazioni o conversazioni può essere appreso da altri a causa del tipo di apparecchiature terminali utilizzate o del collegamento realizzato tra le stesse presso la sede dell'abbonato medesimo.

3. L'utente informa l'altro utente quando, nel corso della conversazione, sono utilizzati dispositivi che consentono l'ascolto della conversazione stessa da parte di altri soggetti.

Art. 132. Conservazione di dati di traffico per altre finalità(1)

1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico, sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione. (2)
1-bis. (3) I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni.

abrogato (4)

2. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-quater del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante.

abrogato (4)
4-bis. [abrogato] (4)
4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle

norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.
4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale.
4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia.

3. (5) Il trattamento dei dati per le finalità di cui al comma 1 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17, volti a garantire che i dati conservati possiedano i medesimi requisiti di qualità, sicurezza e protezione dei dati in rete, nonché a:

   (a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'allegato B);

soppressa (6)

soppressa (6)

(b) indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui al comma 1.

(1) Articolo così modificato, inizialmente, dal decreto-legge 24 dicembre 2003, n. 354, convertito dalla legge 26 febbraio 2004, n. 45, recante interventi per l'amministrazione della giustizia; poi dal decreto-legge 27 luglio 2005, n. 144, convertito dalla legge 31 luglio 2005, n. 155, recante misure urgenti per il contrasto del terrorismo internazionale; successivamente, dalla legge 18 marzo 2008, n. 48, recante ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno; e, da ultimo, dal decreto legislativo 30 maggio 2008, n. 109, di attuazione della direttiva 2006/24/Ce riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/Ce. Al fine di delineare con completezza il quadro normativo vigente in materia, si riporta l'articolo 6, comma 1, e 7 del decreto-legge del 27 luglio 2005, n. 144 Misure urgenti per il contrasto del terrorismo internazionale, come modificato dal decreto-legge del 31 dicembre 2007, n. 248, convertito, con modificazioni, dalla legge n. 31 del 27 febbraio 2008:

6. Nuove norme sui dati del traffico telefonico e telematico

1. A decorrere dalla data di entrata in vigore del presente decreto e fino alla data di entrata in vigore del provvedimento legislativo di attuazione della direttiva 2006/24/Ce del Parlamento europeo e del Consiglio, del 15 marzo 2006, e comunque non oltre il 31 dicembre 2008, è sospesa l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni e limitatamente alle informazioni che consentono la tracciabilità degli accessi, nonché, qualora disponibili, dei servizi, debbono essere conservati fino alla data di entrata in vigore del provvedimento legislativo di attuazione della direttiva 2006/24/Ce del Parlamento europeo e del Consiglio, del 15 marzo 2006, e comunque non oltre il 31 dicembre 2008, dai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, fatte salve le disposizioni vigenti che prevedono un periodo di conservazione ulteriore. I dati del traffico conservati oltre i limiti previsti dall'articolo 132 del decreto legislativo 30 giugno 2003, n. 196, possono essere utilizzati esclusivamente per le finalità del presente decreto, salvo l'esercizio dell'azione penale per i reati comunque perseguibili.

7. Integrazione della disciplina amministrativa degli esercizi pubblici di telefonia e Internet

1. A decorrere dal quindicesimo giorno successivo alla data di entrata in vigore della legge di conversione del presente decreto e fino al 31 dicembre 2008, chiunque intende aprire un pubblico esercizio o un circolo privato di qualsiasi specie, nel quale sono posti a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni anche telematiche, deve chiederne la licenza al questore. La licenza non è richiesta nel caso di sola installazione di telefoni pubblici a pagamento, abilitati esclusivamente alla telefonia vocale.

2. Per coloro che già esercitano le attività di cui al comma 1, la licenza deve essere richiesta entro sessanta giorni dalla data di entrata in vigore del presente decreto.

(2) Comma così modificato prima dall'art. 6, d.l. 27 luglio 2005, n. 144 e poi dall'art. 2 d.lg. 30 maggio 2008, n. 109.

(3) Il comma 1-bis, introdotto dall'articolo 2, comma 1, lett. b), del d.lg. 30 maggio 2008, n. 109, ha effetto decorsi

tre mesi dalla sua data di entrata in vigore (art. 6, comma 3, d.lg. 109/2008).

(4) Così abrogati dall'art. 2, comma 1, lettera c), d.lg. 109/2008.

(5) Così modificato dall'art. 2, comma 1, lettera d), d.lg. 109/2008.

(6) Così soppresse dall'art. 2, comma 1, lettera d), punto 2, d.lg. 109/2008.

Capo II - Internet e reti telematiche

Art. 133. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato da fornitori di servizi di comunicazione e informazione offerti mediante reti di comunicazione elettronica, con particolare riguardo ai criteri per assicurare ed uniformare una più adeguata informazione e consapevolezza degli utenti delle reti di comunicazione elettronica gestite da soggetti pubblici e privati rispetto ai tipi di dati personali trattati e alle modalità del loro trattamento, in particolare

attraverso informative fornite in linea in modo agevole e interattivo, per favorire una più ampia trasparenza e correttezza nei confronti dei medesimi utenti e il pieno rispetto dei principi di cui all'articolo 11, anche ai fini dell'eventuale rilascio di certificazioni attestanti la qualità delle modalità prescelte e il livello di sicurezza assicurato.

Capo III - Videosorveglianza

Art. 134. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantire la liceità e la correttezza anche in riferimento a quanto previsto dall'articolo 11.

A.2.11 Titolo XI - Libere professioni e investigazione privata

Capo I - Profili generali

Art. 135. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o per far valere o difendere un diritto in sede giudiziaria, in particolare da liberi professionisti o da soggetti che esercitano un'attività di investigazione privata autorizzata in conformità alla legge.

A.2.12 Titolo XII - Giornalismo ed espressione letteraria ed artistica

Capo I - Profili generali

Art. 136. Finalità giornalistiche e altre manifestazioni del pensiero

1. Le disposizioni del presente titolo si applicano al trattamento:

   (a) effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità;

   (b) effettuato dai soggetti iscritti nell'elenco dei pubblicisti o nel registro dei praticanti di cui agli articoli 26 e 33 della legge 3 febbraio 1963, n. 69;

   (c) temporaneo finalizzato esclusivamente alla pubblicazione o diffusione occasionale di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica.

Art. 137. Disposizioni applicabili

1. Ai trattamenti indicati nell'articolo 136 non si applicano le disposizioni del presente codice relative:

   (a) all'autorizzazione del Garante prevista dall'articolo 26;

   (b) alle garanzie previste dall'articolo 27 per i dati giudiziari;

   (c) al trasferimento dei dati all'estero, contenute nel Titolo VII della Parte I.

2. Il trattamento dei dati di cui al comma 1 è effettuato anche senza il consenso dell'interessato previsto dagli articoli 23 e 26.

3. In caso di diffusione o di comunicazione dei dati per le finalità di cui all'articolo 136 restano fermi i limiti del diritto di cronaca a tutela dei diritti di cui all'articolo 2 e, in particolare, quello dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico. Possono essere trattati i dati personali relativi a circostanze o fatti resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico.

Art. 138. Segreto professionale

1. In caso di richiesta dell'interessato di conoscere l'origine dei dati personali ai sensi dell'articolo 7, comma 2, lettera a) restano ferme le norme sul segreto professionale degli esercenti la professione di giornalista, limitatamente alla fonte della notizia.

Capo II - Codice di deontologia

Art. 139. Codice di deontologia relativo ad attività giornalistiche

1. Il Garante promuove ai sensi dell'articolo 12 l'adozione da parte del Consiglio nazionale dell'ordine dei giornalisti di un codice di deontologia relativo al trattamento dei dati di cui all'articolo 136, che prevede misure ed accorgimenti a garanzia degli interessati rapportate alla natura dei dati, in particolare per quanto riguarda quelli idonei a rivelare lo stato di salute e la vita sessuale. Il codice può anche prevedere forme semplificate per le informative di cui all'articolo 13.

2. Nella fase di formazione del codice, ovvero successivamente, il Garante, in cooperazione con il Consiglio, prescrive eventuali misure e accorgimenti a garanzia degli interessati, che il Consiglio è tenuto a recepire.

3. Il codice o le modificazioni od integrazioni al codice di deontologia che non sono adottati dal Consiglio entro sei mesi dalla proposta del Garante sono adottati in via sostitutiva dal Garante e sono efficaci sino a quando diviene efficace una diversa disciplina secondo la procedura di cooperazione.

4. Il codice e le disposizioni di modificazione ed integrazione divengono efficaci quindici giorni dopo la loro pubblicazione nella Gazzetta Ufficiale ai sensi dell'articolo 12.

5. In caso di violazione delle prescrizioni contenute nel codice di deontologia, il Garante può vietare il trattamento ai sensi dell'articolo 143, comma 1, lettera c).

A.2.13 Titolo XIII - Marketing diretto

Capo I - Profili generali

Art. 140. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale, prevedendo anche, per i casi in cui il trattamento non presuppone il consenso dell'interessato, forme semplificate per manifestare e rendere meglio conoscibile l'eventuale dichiarazione di non voler ricevere determinate comunicazioni.

A.3 Parte III - Tutela dell'interessato e sanzioni

A.3.1 Titolo I - Tutela amministrativa e giurisdizionale

Capo I - Tutela dinnanzi al Garante
Sezione I - Principi generali

Art. 141. Forme di tutela

1. L'interessato può rivolgersi al Garante:
   (a) mediante reclamo circostanziato nei modi previsti dall'articolo 142, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali;
   (b) mediante segnalazione, se non è possibile presentare un reclamo circostanziato ai sensi della lettera a), al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima;
   (c) mediante ricorso, se intende far valere gli specifici diritti di cui all'articolo 7 secondo le modalità e per conseguire gli effetti previsti nella sezione III del presente capo.

Sezione II - Tutela amministrativa

Art. 142. Proposizione dei reclami

1. Il reclamo contiene un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonché gli estremi identificativi del titolare, del responsabile, ove conosciuto, e dell'istante.

2. Il reclamo è sottoscritto dagli interessati, o da associazioni che li rappresentano anche ai sensi dell'articolo 9, comma 2, ed è presentato al Garante senza particolari formalità. Il reclamo reca in allegato la documentazione utile ai fini della sua valutazione e l'eventuale procura, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica, telefax o telefono.

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

Art. 143. Procedimento per i reclami

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

   (a) prima di prescrivere le misure di cui alla lettera b), ovvero il divieto o il blocco ai sensi della lettera c), può invitare il titolare, anche in contraddittorio con l'interessato, ad effettuare il blocco spontaneamente;

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

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

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

2. I provvedimenti di cui al comma 1 sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana se i relativi destinatari non sono facilmente identificabili per il numero o per la complessità degli accertamenti.

Art. 144. Segnalazioni

1. I provvedimenti di cui all'articolo 143 possono essere adottati anche a seguito delle segnalazioni di cui all'articolo 141, comma 1, lettera b), se è avviata un'istruttoria preliminare e anche prima della definizione del procedimento.

Sezione III - Tutela alternativa a quella giurisdizionale

Art. 145. Ricorsi

1. I diritti di cui all'articolo 7 possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante.

2. Il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria.

3. La presentazione del ricorso al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto.

Art. 146. Interpello preventivo

1. Salvi i casi in cui il decorso del termine esporrebbe taluno a pregiudizio imminente ed irreparabile, il ricorso al Garante può essere proposto solo dopo che è stata avanzata richiesta sul medesimo oggetto al titolare o al responsabile ai sensi dell'articolo 8, comma 1, e sono decorsi i termini previsti dal presente articolo, ovvero è stato opposto alla richiesta un diniego anche parziale.

2. Il riscontro alla richiesta da parte del titolare o del responsabile è fornito entro quindici giorni dal suo ricevimento.

3. Entro il termine di cui al comma 2, se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessità, ovvero ricorre altro giustificato motivo, il titolare o il responsabile ne danno comunicazione all'interessato. In tal caso, il termine per l'integrale riscontro è di trenta giorni dal ricevimento della richiesta medesima.

Art. 147. Presentazione del ricorso

1. Il ricorso è proposto nei confronti del titolare e indica:

   (a) gli estremi identificativi del ricorrente, dell'eventuale procuratore speciale, del titolare e, ove conosciuto, del responsabile eventualmente designato per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7;

   (b) la data della richiesta presentata al titolare o al responsabile ai sensi dell'articolo 8, comma 1, oppure del pregiudizio imminente ed irreparabile che permette di prescindere dalla richiesta medesima;

   (c) gli elementi posti a fondamento della domanda;

   (d) il provvedimento richiesto al Garante;

   (e) il domicilio eletto ai fini del procedimento.

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

   (a) la copia della richiesta rivolta al titolare o al responsabile ai sensi dell'articolo 8, comma 1;

   (b) l'eventuale procura;

   (c) la prova del versamento dei diritti di segreteria.

3. Al ricorso è unita, altresì, la documentazione utile ai fini della sua valutazione e l'indicazione di un recapito per l'invio di comunicazioni al ricorrente o al procuratore speciale mediante posta elettronica, telefax o telefono.

4. Il ricorso è rivolto al Garante e la relativa sottoscrizione è autenticata. L'autenticazione non è richiesta se la sottoscrizione è apposta presso l'Ufficio del Garante o da un procuratore speciale iscritto all'albo degli avvocati al quale la procura è conferita ai sensi dell'articolo 83 del codice di procedura civile, ovvero con firma digitale in conformità alla normativa vigente.

5. Il ricorso è validamente proposto solo se è trasmesso con plico raccomandato, oppure per via telematica osservando le modalità relative alla sottoscrizione con firma digitale e alla conferma del ricevimento prescritte ai sensi dell'articolo 38, comma 2, ovvero presentato direttamente presso l'Ufficio del Garante.

Art. 148. Inammissibilità del ricorso

1. Il ricorso è inammissibile:

   (a) se proviene da un soggetto non legittimato;

   (b) in caso di inosservanza delle disposizioni di cui agli articoli 145 e 146;

   (c) se difetta di taluno degli elementi indicati nell'articolo 147, commi 1 e 2, salvo che sia regolarizzato dal ricorrente o dal procuratore speciale anche su invito dell'Ufficio del Garante ai sensi del comma 2, entro sette giorni dalla data della sua presentazione o della ricezione dell'invito. In tale caso, il ricorso si considera presentato al momento in cui il ricorso regolarizzato perviene all'Ufficio.

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

Art. 149. Procedimento relativo al ricorso

1. Fuori dei casi in cui è dichiarato inammissibile o manifestamente infondato, il ricorso è comunicato al titolare entro tre giorni a cura dell'Ufficio del Garante, con invito ad esercitare entro dieci giorni dal suo ricevimento la facoltà di comunicare al ricorrente e all'Ufficio la propria eventuale adesione spontanea. L'invito è comunicato al titolare per il tramite del responsabile eventualmente designato per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, ove indicato nel ricorso.

2. In caso di adesione spontanea è dichiarato non luogo a provvedere. Se il ricorrente lo richiede, è determinato in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso, posti a carico della controparte o compensati per giusti motivi anche parzialmente.

3. Nel procedimento dinanzi al Garante il titolare, il responsabile di cui al comma 1 e l'interessato hanno diritto di essere sentiti, personalmente o a mezzo di procuratore speciale, e hanno facoltà di presentare memorie o documenti. A tal fine l'invito di cui al comma 1 è trasmesso anche al ricorrente e reca l'indicazione del termine entro il quale il titolare, il medesimo responsabile e l'interessato possono presentare memorie e documenti, nonché della data in cui tali soggetti possono essere sentiti in contraddittorio anche mediante idonea tecnica audiovisiva.

4. Nel procedimento il ricorrente può precisare la domanda nei limiti di quanto chiesto con il ricorso o a seguito di eccezioni formulate dal titolare.

5. Il Garante può disporre, anche d'ufficio, l'espletamento di una o più perizie. Il provvedimento che le dispone precisa il contenuto dell'incarico e il termine per la sua esecuzione, ed è comunicato alle parti le quali possono presenziare alle operazioni personalmente o tramite procuratori o consulenti designati. Il provvedimento dispone inoltre in ordine all'anticipazione delle spese della perizia.

6. Nel procedimento, il titolare e il responsabile di cui al comma 1 possono essere assistiti da un procuratore o da altra persona di fiducia.

7. Se gli accertamenti risultano particolarmente complessi o vi è l'assenso delle parti il termine di sessanta giorni di cui all'articolo 150, comma 2, può essere prorogato per un periodo non superiore ad ulteriori quaranta giorni.

8. Il decorso dei termini previsti dall'articolo 150, comma 2 e dall'articolo 151 è sospeso di diritto dal 1 agosto al 15 settembre di ciascun anno e riprende a decorrere dalla fine del periodo di sospensione. Se il decorso ha inizio durante tale periodo, l'inizio stesso è differito alla fine del periodo medesimo. La sospensione non opera nei casi in cui sussiste il pregiudizio di cui all'articolo 146, comma 1, e non preclude l'adozione dei provvedimenti di cui all'articolo 150, comma 1.

Art. 150. Provvedimenti a seguito del ricorso

1. Se la particolarità del caso lo richiede, il Garante può disporre in via provvisoria il blocco in tutto o in parte di taluno dei dati, ovvero l'immediata sospensione di una o più operazioni del trattamento. Il provvedimento può essere adottato anche prima della comunicazione del ricorso ai sensi dell'articolo 149, comma 1, e cessa di avere ogni effetto se non è adottata nei termini la decisione di cui al comma 2. Il medesimo provvedimento è impugnabile unitamente a tale decisione.

2. Assunte le necessarie informazioni il Garante, se ritiene fondato il ricorso, ordina al titolare, con decisione motivata, la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione. La mancata pronuncia sul ricorso, decorsi sessanta giorni dalla data di presentazione, equivale a rigetto.

3. Se vi è stata previa richiesta di taluna delle parti, il provvedimento che definisce il procedimento determina in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso, posti a carico, anche in parte, del soccombente o compensati anche parzialmente per giusti motivi.

4. Il provvedimento espresso, anche provvisorio, adottato dal Garante è comunicato alle parti entro dieci giorni presso il domicilio eletto o risultante dagli atti. Il provvedimento può essere comunicato alle parti anche mediante posta elettronica o telefax.

5. Se sorgono difficoltà o contestazioni riguardo all'esecuzione del provvedimento di cui ai commi 1 e 2, il Garante, sentite le parti ove richiesto, dispone le modalità di attuazione avvalendosi, se necessario, del personale dell'Ufficio o della collaborazione di altri organi dello Stato.

6. In caso di mancata opposizione avverso il provvedimento che determina l'ammontare delle spese e dei diritti, o di suo rigetto, il provvedimento

medesimo costituisce, per questa parte, titolo esecutivo ai sensi degli articoli 474 e 475 del codice di procedura civile.

Art. 151. Opposizione

1. Avverso il provvedimento espresso o il rigetto tacito di cui all'articolo 150, comma 2, il titolare o l'interessato possono proporre opposizione con ricorso ai sensi dell'articolo 152. L'opposizione non sospende l'esecuzione del provvedimento.

2. Il tribunale provvede nei modi di cui all'articolo 152.

Capo II - Tutela giurisdizionale

Art. 152. Autorità giudiziaria ordinaria

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

2. Per tutte le controversie di cui al comma 1 l'azione si propone con ricorso depositato nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento.

3. Il tribunale decide in ogni caso in composizione monocratica.

4. Se è presentato avverso un provvedimento del Garante anche ai sensi dell'articolo 143, il ricorso è proposto entro il termine di trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito. Se il ricorso è proposto oltre tale termine il giudice lo dichiara inammissibile con ordinanza ricorribile per cassazione.

5. La proposizione del ricorso non sospende l'esecuzione del provvedimento del Garante. Se ricorrono gravi motivi il giudice, sentite le parti, può disporre diversamente in tutto o in parte con ordinanza impugnabile unitamente alla decisione che definisce il grado di giudizio.

6. Quando sussiste pericolo imminente di un danno grave ed irreparabile il giudice può emanare i provvedimenti necessari con decreto motivato, fissando, con il medesimo provvedimento, l'udienza di comparizione delle parti entro un termine non superiore a quindici giorni. In tale udienza, con ordinanza, il giudice conferma, modifica o revoca i provvedimenti emanati con decreto.

7. Il giudice fissa l'udienza di comparizione delle parti con decreto con il quale assegna al ricorrente il termine perentorio entro cui notificarlo alle altre parti e al Garante. Tra il giorno della notificazione e l'udienza di comparizione intercorrono non meno di trenta giorni.

8. Se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impedimento, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio.

9. Nel corso del giudizio il giudice dispone, anche d'ufficio, omettendo ogni formalità non necessaria al contraddittorio, i mezzi di prova che ritiene necessari e può disporre la citazione di testimoni anche senza la formulazione di capitoli.

10. Terminata l'istruttoria, il giudice invita le parti a precisare le conclusioni ed a procedere, nella stessa udienza, alla discussione orale della causa, pronunciando subito dopo la sentenza mediante lettura del dispositivo. Le motivazioni della sentenza sono depositate in cancelleria entro i successivi trenta giorni. Il giudice può anche redigere e leggere, unitamente al dispositivo, la motivazione della sentenza, che è subito dopo depositata in cancelleria.

11. Se necessario, il giudice può concedere alle parti un termine non superiore a dieci giorni per il deposito di note difensive e rinviare la causa all'udienza immediatamente successiva alla scadenza del termine per la discussione e la pronuncia della sentenza.

12. Con la sentenza il giudice, anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), quando è necessario anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile, accoglie o rigetta la domanda, in tutto o in parte, prescrive le misure necessarie, dispone sul risarcimento del danno, ove richiesto, e pone a carico della parte soccombente le spese del procedimento.

13. La sentenza non è appellabile, ma è ammesso il ricorso per cassazione.

14. Le disposizioni di cui al presente articolo si applicano anche nei casi previsti dall'articolo 10, comma 5, della legge 1 aprile 1981, n. 121, e successive modificazioni.

A.3.2 Titolo II - L'Autorità

Capo I - Il Garante per la protezione dei dati personali

Art. 153. Il Garante

1. Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione.

2. Il Garante è organo collegiale costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. I componenti sono scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni.

3. I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. Eleggono altresì un vicepresidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.

4. (2) 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 il presidente e i componenti non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive.

5. All'atto dell'accettazione della nomina il presidente e i componenti sono collocati fuori ruolo se dipendenti di pubbliche amministrazioni o magistrati in attività di servizio; se professori universitari di ruolo, sono collocati in aspettativa senza assegni ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni. Il personale collocato fuori ruolo o in aspettativa non può essere sostituito.

6. Al presidente compete una indennità di funzione non eccedente, nel massimo, la retribuzione spettante al primo presidente della Corte di cassazione. Ai componenti compete un'indennità non eccedente nel massimo, i due terzi di quella spettante al presidente. Le predette indennità di funzione sono determinate dall'articolo 6 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501, in misura tale da poter essere corrisposte a carico degli ordinari stanziamenti.

7. Alle dipendenze del Garante è posto l'Ufficio di cui all'articolo 156.

(2) L'art. 47-quater decreto legge n. 248 del 31 dicembre 2007, convertito con modificazioni dalla legge n. 31 del 27 febbraio 2008, ha equiparato la durata in carica del presidente e dei componenti del Garante a quella di sette anni, prevista per altre autorità indipendenti, con decorrenza dalla data del decreto di nomina. Gli incarichi non sono rinnovabili.

Art. 154. Compiti

1. Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di:

   (a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione, anche in caso di loro cessazione e con riferimento alla conservazione dei dati di traffico; (1)

   (b) esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano;

   (c) prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143;

   (d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco ai sensi dell'articolo 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;

   (e) promuovere la sottoscrizione di codici ai sensi dell'articolo 12 e dell'articolo 139;

   (f) segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti di cui all'articolo 2 anche a seguito dell'evoluzione del settore;

   (g) esprimere pareri nei casi previsti;

   (h) curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati;

   (i) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;

(j) tenere il registro dei trattamenti formato sulla base delle notificazioni di cui all'articolo 37;

(k) predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione del presente codice, che è trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce.

2. Il Garante svolge altresì, ai sensi del comma 1, la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da regolamenti comunitari e, in particolare:

(a) dalla legge 30 settembre 1993, n. 388, e successive modificazioni, di ratifica ed esecuzione dei protocolli e degli accordi di adesione all'accordo di Schengen e alla relativa convenzione di applicazione;

(b) dalla legge 23 marzo 1998, n. 93, e successive modificazioni, di ratifica ed esecuzione della convenzione istitutiva dell'Ufficio europeo di polizia (Europol);

(c) dal regolamento (Ce) n. 515/97 del Consiglio, del 13 marzo 1997, e dalla legge 30 luglio 1998, n. 291, e successive modificazioni, di ratifica ed esecuzione della convenzione sull'uso dell'informatica nel settore doganale;

(d) dal regolamento (Ce) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'Eurodac per il confronto delle impronte digitali e per l'efficace applicazione della convenzione di Dublino;

(e) nel capitolo IV della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della convenzione medesima.

3. Il Garante coopera con altre autorità amministrative indipendenti nello svolgimento dei rispettivi compiti. A tale fine, il Garante può anche invitare rappresentanti di un'altra autorità a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorità, prendendo parte alla discussione di argomenti di comune interesse; può richiedere, altresì, la collaborazione di personale specializzato addetto ad altra autorità.

4. Il Presidente del Consiglio dei ministri e ciascun ministro consultano il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dal presente codice.

5. Fatti salvi i termini più brevi previsti per legge, il parere del Garante è reso nei casi previsti nel termine di quarantacinque giorni dal ricevimento della richiesta. Decorso il termine, l'amministrazione può procedere indipendentemente dall'acquisizione del parere. Quando, per esigenze istruttorie, non può essere rispettato il termine di cui al presente comma, tale termine può essere interrotto per una sola volta e il parere deve essere reso definitivamente entro venti giorni dal ricevimento degli elementi istruttori da parte delle amministrazioni interessate.

6. Copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal presente codice o in materia di criminalità informatica è trasmessa, a cura della cancelleria, al Garante.

(1) Lettera così modificata dall'art. 4, decreto legislativo 30 maggio 2008, n. 109, di attuazione della direttiva 2006/24/Ce riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/Ce.

Capo II - L'Ufficio del Garante

Art. 155. Principi applicabili

1. All'Ufficio del Garante, al fine di garantire la responsabilità e l'autonomia ai sensi della legge 7 agosto 1990, n. 241, e successive modificazioni, e del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, si applicano i principi riguardanti l'individuazione e le funzioni del responsabile del procedimento, nonché quelli relativi alla distinzione fra le funzioni di indirizzo e di controllo, attribuite agli organi di vertice, e le funzioni di gestione attribuite ai dirigenti. Si applicano altresì le disposizioni del medesimo decreto legislativo n. 165 del 2001 espressamente richiamate dal presente codice.

Art. 156. Ruolo organico e personale

1. All'Ufficio del Garante è preposto un segretario generale scelto anche tra magistrati ordinari o amministrativi.

2. Il ruolo organico del personale dipendente è stabilito nel limite di cento unità.

3. Con propri regolamenti pubblicati nella Gazzetta Ufficiale della Repubblica italiana, il Garante definisce:

   (a) l'organizzazione e il funzionamento dell'Ufficio anche ai fini dello svolgimento dei compiti di cui all'articolo 154;

   (b) l'ordinamento delle carriere e le modalità di reclutamento del personale secondo le procedure previste dall'articolo 35 del decreto legislativo n. 165 del 2001;

   (c) la ripartizione dell'organico tra le diverse aree e qualifiche;

   (d) il trattamento giuridico ed economico del personale, secondo i criteri previsti dalla legge 31 luglio 1997, n. 249, e successive modificazioni e, per gli incarichi dirigenziali, dagli articoli 19, comma 6, e 23-bis del decreto legislativo 30 marzo 2001, n. 165, tenuto conto delle specifiche esigenze funzionali e organizzative. Nelle more della più generale razionalizzazione del trattamento economico delle autorità amministrative indipendenti, al personale è attribuito l'ottanta per cento del trattamento economico del personale dell'Autorità per le garanzie nelle comunicazioni;

   (e) la gestione amministrativa e la contabilità, anche in deroga alle norme sulla contabilità generale dello Stato, l'utilizzo dell'avanzo di amministrazione nel quale sono iscritte le somme già versate nella contabilità speciale, nonché l'individuazione dei casi di riscossione e utilizzazione dei diritti di segreteria o di corrispettivi per servizi resi in base a disposizioni di legge secondo le modalità di cui all'articolo 6, comma 2, della legge 31 luglio 1997, n. 249.

4. L'Ufficio può avvalersi, per motivate esigenze, di dipendenti dello Stato o di altre amministrazioni pubbliche o di enti pubblici collocati in posizione di fuori ruolo o equiparati nelle forme previste dai rispettivi ordinamenti, ovvero in aspettativa ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni, in numero non superiore, complessivamente, a venti unità e per non oltre il venti per cento delle qualifiche dirigenziali, lasciando non coperto un corrispondente numero di posti di ruolo. Al personale di cui al presente comma è corrisposta un'indennità pari all'eventuale

differenza tra il trattamento erogato dall'amministrazione o dall'ente di provenienza e quello spettante al personale di ruolo, sulla base di apposita tabella di corrispondenza adottata dal Garante, e comunque non inferiore al cinquanta per cento della retribuzione in godimento, con esclusione dell'indennità integrativa speciale.

5. In aggiunta al personale di ruolo, l'Ufficio può assumere direttamente dipendenti con contratto a tempo determinato, in numero non superiore a venti unità ivi compresi i consulenti assunti con contratto a tempo determinato ai sensi del comma 7.

6. Si applicano le disposizioni di cui all'articolo 30 del decreto legislativo n. 165 del 2001.

7. Nei casi in cui la natura tecnica o la delicatezza dei problemi lo richiedono, il Garante può avvalersi dell'opera di consulenti, i quali sono remunerati in base alle vigenti tariffe professionali ovvero sono assunti con contratti a tempo determinato, di durata non superiore a due anni, che possono essere rinnovati per non più di due volte.

8. Il personale addetto all'Ufficio del Garante ed i consulenti sono tenuti al segreto su ciò di cui sono venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete.

9. Il personale dell'Ufficio del Garante addetto agli accertamenti di cui all'articolo 158 riveste, in numero non superiore a cinque unità, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, la qualifica di ufficiale o agente di polizia giudiziaria.

10. Le spese di funzionamento del Garante sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposito capitolo dello stato di previsione del Ministero dell'economia e delle finanze. Il rendiconto della gestione finanziaria è soggetto al controllo della Corte dei conti.

Capo III - Accertamenti e controlli

Art. 157. Richiesta di informazioni e di esibizione di documenti

1. Per l'espletamento dei propri compiti il Garante può richiedere al titolare, al responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti.

Art. 158. Accertamenti

1. Il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

2. I controlli di cui al comma 1 sono eseguiti da personale dell'Ufficio. Il Garante si avvale anche, ove necessario, della collaborazione di altri organi dello Stato.

3. Gli accertamenti di cui al comma 1, se svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze, sono effettuati con l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al più tardi entro tre giorni dal ricevimento della richiesta del Garante quando è documentata l'indifferibilità dell'accertamento.

Art. 159. Modalità

1. Il personale operante, munito di documento di riconoscimento, può essere assistito ove necessario da consulenti tenuti al segreto ai sensi dell'articolo 156, comma 8. Nel procedere a rilievi e ad operazioni tecniche può altresì estrarre copia di ogni atto, dato e documento, anche a campione e su supporto informatico o per via telematica. Degli accertamenti è redatto sommario verbale nel quale sono annotate anche le eventuali dichiarazioni dei presenti.

2. Ai soggetti presso i quali sono eseguiti gli accertamenti è consegnata copia dell'autorizzazione del presidente del tribunale, ove rilasciata. I medesimi soggetti sono tenuti a farli eseguire e a prestare la collaborazione a tal fine necessaria. In caso di rifiuto gli accertamenti sono comunque eseguiti e le spese in tal caso occorrenti sono poste a carico del titolare con il provvedimento che definisce il procedimento, che per questa parte costituisce titolo esecutivo ai sensi degli articoli 474 e 475 del codice di procedura civile.

3. Gli accertamenti, se effettuati presso il titolare o il responsabile, sono eseguiti dandone informazione a quest'ultimo o, se questo è assente o

non è designato, agli incaricati. Agli accertamenti possono assistere persone indicate dal titolare o dal responsabile.

4. Se non è disposto diversamente nel decreto di autorizzazione del presidente del tribunale, l'accertamento non può essere iniziato prima delle ore sette e dopo le ore venti, e può essere eseguito anche con preavviso quando ciò può facilitarne l'esecuzione.

5. Le informative, le richieste e i provvedimenti di cui al presente articolo e agli articoli 157 e 158 possono essere trasmessi anche mediante posta elettronica e telefax.

6. Quando emergono indizi di reato si osserva la disposizione di cui all'articolo 220 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271.

Art. 160. Particolari accertamenti

1. Per i trattamenti di dati personali indicati nei titoli I, II e III della Parte II gli accertamenti sono effettuati per il tramite di un componente designato dal Garante.

2. Se il trattamento non risulta conforme alle disposizioni di legge o di regolamento, il Garante indica al titolare o al responsabile le necessarie modificazioni ed integrazioni e ne verifica l'attuazione. Se l'accertamento è stato richiesto dall'interessato, a quest'ultimo è fornito in ogni caso un riscontro circa il relativo esito, se ciò non pregiudica azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione di reati o ricorrono motivi di difesa o di sicurezza dello Stato.

3. Gli accertamenti non sono delegabili. Quando risulta necessario in ragione della specificità della verifica, il componente designato può farsi assistere da personale specializzato tenuto al segreto ai sensi dell'articolo 156, comma 8. Gli atti e i documenti acquisiti sono custoditi secondo modalità tali da assicurarne la segretezza e sono conoscibili dal presidente e dai componenti del Garante e, se necessario per lo svolgimento delle funzioni dell'organo, da un numero delimitato di addetti all'Ufficio individuati dal Garante sulla base di criteri definiti dal regolamento di cui all'articolo 156, comma 3, lettera a).

4. Per gli accertamenti relativi agli organismi di informazione e di sicurezza e ai dati coperti da segreto di Stato il componente designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante.

5. Nell'effettuare gli accertamenti di cui al presente articolo nei riguardi di uffici giudiziari, il Garante adotta idonee modalità nel rispetto delle reciproche attribuzioni e della particolare collocazione istituzionale dell'organo procedente. Gli accertamenti riferiti ad atti di indagine coperti dal segreto sono differiti, se vi è richiesta dell'organo procedente, al momento in cui cessa il segreto.

6. La validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale.

A.3.3 Sanzioni

Capo I - Violazioni amministrative

Art. 161. Omessa o inidonea informativa all'interessato (1)
1. La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da seimila euro a trentaseimila euro.

(1) Così modificato dalla legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del decreto-legge n. 207 del 30 dicembre 2008

Art. 162. Altre fattispecie
1. La cessione dei dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera b), o di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro (1).
2. La violazione della disposizione di cui all'articolo 84, comma 1, è punita con la sanzione amministrativa del pagamento di una somma da mille euro a seimila euro (1).
2-bis. (2) In caso di trattamento di dati personali effettuato in violazione delle misure indicate nell'articolo 33 o delle disposizioni indicate nell'articolo 167 è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da diecimila euro (3) a centoventimila euro. Nei

casi di cui all'articolo 33 è escluso il pagamento in misura ridotta.
2-ter. (2) In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro.
2-quater. (4) La violazione del diritto di opposizione nelle forme previste dall'articolo 130, comma 3-bis, e dal relativo regolamento è sanzionata ai sensi del comma 2-bis del presente articolo.

(1) Così modificato
(2) Comma così aggiunto dalla legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del decreto-legge n. 207 del 30 dicembre 2008
(3) Comma così modificato dal n. 1) della lettera c) del comma 1 dell'art. 20-bis, D.L. 25 settembre 2009, n. 135, nel testo integrato dalla relativa legge di conversione 20 novembre 2009, n. 166.
(4) Comma aggiunto dal n. 2) della lettera c) del comma 1 dell'art. 20-bis, D.L. 25 settembre 2009, n. 135, nel testo integrato dalla relativa legge di conversione 20 novembre 2009, n. 166.

Al fine di delineare con completezza il quadro normativo vigente in materia, si riportano i commi 2, 3 e 4 dell'art. 20-bis della legge 20 novembre 2009, n. 166 di conversione, con modificazioni, del D.L.25 settembre 2009, n. 135.

2. Il registro previsto dall' articolo 130, comma 3-bis, del codice d cui al decreto legislativo 30 giugno 2003, n. 196, introdotto dal comma 1, lettera b), del presente articolo, è istituito entro sei mesi dalla data di entrata in vigore della legge di conversione del presente decreto. Fino al suddetto termine, restano in vigore i provvedimenti adottati dal Garante per la protezione dei dati personali ai sensi dell' articolo 154 del citato codice di cui al decreto legislativo n. 196 del 2003, e successive modificazioni, in attuazione dell' articolo 129 del medesimo codice.

3. All' articolo 44, comma 1-bis, del decreto-legge 30 dicembre 2008, n. 207, convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14, le parole: sino al 31 dicembre 2009 sono sostituite dalle seguenti: sino al termine di sei mesi successivi alla data di entrata in vigore della legge di conversione del decreto-legge 25 settembre 2009, n. 135.

4. All' articolo 58 del codice del consumo, di cui al decreto legislativo 6 settembre 2005, n. 206, il comma 1 è sostituito dal seguente:
1. L'impiego da parte di un professionista del telefono, della posta elettronica, di sistemi automatizzati di chiamata senza l'intervento di un operatore o di fax richiede il consenso preventivo del consumatore, fatta salva la disciplina prevista dall' articolo 130, comma 3-bis, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, per i trattamenti dei dati inclusi negli elenchi di abbonati a disposizione del pubblico.

Art. 162-bis. Sanzioni in materia di conservazione dei dati di traffico (1)
1. Salvo che il fatto costituisca reato e salvo quanto previsto dall'articolo 5, comma 2, del decreto legislativo di recepimento della direttiva 2006/24/Ce del Parlamento europeo e del Consiglio del 15 marzo 2006, nel caso di violazione delle disposizioni di cui all'art. 132, commi 1 e 1-bis, si applica la sanzione amministrativa pecuniaria da 10.000 euro a 50.000 euro. (2)

(1) Articolo aggiunto dall'art. 5, comma 1, del d.lg. 30 maggio 2008, n. 109, di attuazione della direttiva 2006/24/Ce riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/Ce. Per completezza, si riporta il comma 2 del predetto articolo 5, richiamato dall'articolo 162-bis del Codice:

2. Salvo che il fatto costituisca reato, l'omessa o l'incompleta conservazione dei dati ai sensi dell'articolo 132, commi 1 e 1-bis, del Codice, è punita con la sanzione amministrativa pecuniaria da euro 10.000 ad euro 50.000 che può essere aumentata fino al triplo in ragione delle condizioni economiche dei responsabili della violazione. Nel caso di assegnazione di indirizzo IP che non consente l'identificazione univoca dell'utente o abbonato si applica la sanzione amministrativa pecuniaria da 5.000 euro a 50.000 euro, che può essere aumentata fino al triplo in ragione delle condizioni economiche dei responsabili della violazione. Le violazioni sono contestate e le sanzioni sono applicate dal Ministero dello sviluppo economico..

(2) Così modificato dalla legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del decreto-legge n. 207 del 30 dicembre 2008

Art. 163. Omessa o incompleta notificazione (1)
1. Chiunque, essendovi tenuto, non provvede tempestivamente alla notifi-

cazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da ventimila euro a centoventimila euro.

(1) Così modificato dalla legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del decreto-legge n. 207 del 30 dicembre 2008

Art. 164. Omessa informazione o esibizione al Garante (1) 1. Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 150, comma 2, e 157 è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro.

(1) Così modificato dalla legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del decreto-legge n. 207 del 30 dicembre 2008

Art. 164-bis. Casi di minore gravità e ipotesi aggravate (1)
1. Se taluna delle violazioni di cui agli articoli 161, 162, 163 e 164 è di minore gravità, avuto altresì riguardo alla natura anche economica o sociale dell'attività svolta, i limiti minimi e massimi stabiliti dai medesimi articoli sono applicati in misura pari a due quinti.
2. In caso di più violazioni di un'unica o di più disposizioni di cui al presente Capo, a eccezione di quelle previste dagli articoli 162, comma 2, 162-bis e 164, commesse anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni, si applica la sanzione amministrativa del pagamento di una somma da cinquantamila euro a trecentomila euro. Non è ammesso il pagamento in misura ridotta.
3. In altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, i limiti minimo e massimo delle sanzioni di cui al presente Capo sono applicati in misura pari al doppio.
4. Le sanzioni di cui al presente Capo possono essere aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore.

(1) Articolo così aggiunto dalla legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del decreto-legge n. 207 del 30 dicembre 2008

Art. 165. Pubblicazione del provvedimento del Garante (1)
1. Nei casi di cui agli articoli del presente Capo può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione,

per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica. La pubblicazione ha luogo a cura e spese del contravventore.

(1) Così modificato legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del decreto-legge n. 207 del 30 dicembre 2008

Art. 166. Procedimento di applicazione
1. L'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui al presente capo e all'articolo 179, comma 3, è il Garante. Si osservano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689, e successive modificazioni. I proventi, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 156, comma 10, e sono utilizzati unicamente per l'esercizio dei compiti di cui agli articoli 154, comma 1, lettera h), e 158.

Capo II - Illeciti penali

Art. 167. Trattamento illecito di dati
1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

Art. 168. Falsità nelle dichiarazioni e notificazioni al Garante
1. Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

Art. 169. Misure di sicurezza (1)
1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni.

2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

(1) Così modificato legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del decreto-legge n. 207 del 30 dicembre 2008

Art. 170. Inosservanza di provvedimenti del Garante
1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni.

Art. 171. Altre fattispecie
1. La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300.

Art. 172. Pene accessorie
1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza.

A.3.4 Titolo IV - Disposizioni modificative, abrogative, transitorie e finali

Capo I - Dispisizioni di modifica

Art. 173. Convenzione di applicazione dell'Accordo di Schengen

1. La legge 30 settembre 1993, n. 388, e successive modificazioni, di ratifica ed esecuzione dei protocolli e degli accordi di adesione all'accordo di Schengen e alla relativa convenzione di applicazione, è così modificata:

(a) il comma 2 dell'articolo 9 è sostituito dal seguente: 2. Le richieste di accesso, rettifica o cancellazione, nonché di verifica, di cui, rispettivamente, agli articoli 109, 110 e 114, paragrafo 2, della Convenzione, sono rivolte all'autorità di cui al comma 1.;

(b) il comma 2 dell'articolo 10 è soppresso;

(c) l'articolo 11 è sostituito dal seguente: 11. 1. L'autorità di controllo di cui all'articolo 114 della Convenzione è il Garante per la protezione dei dati personali. Nell'esercizio dei compiti ad esso demandati per legge, il Garante esercita il controllo sui trattamenti di dati in applicazione della Convenzione ed esegue le verifiche previste nel medesimo articolo 114, anche su segnalazione o reclamo dell'interessato all'esito di un inidoneo riscontro alla richiesta rivolta ai sensi dell'articolo 9, comma 2, quando non è possibile fornire al medesimo interessato una risposta sulla base degli elementi forniti dall'autorità di cui all'articolo 9, comma 1. 2. Si applicano le disposizioni dell'articolo 10, comma 5, della legge 1 aprile 1981, n. 121, e successive modificazioni.;

(d) l'articolo 12 è abrogato.

Art. 174. Notifiche di atti e vendite giudiziarie

1. 1. All'articolo 137 del codice di procedura civile, dopo il secondo comma, sono inseriti i seguenti:
   Se la notificazione non può essere eseguita in mani proprie del destinatario, tranne che nel caso previsto dal secondo comma dell'articolo 143, l'ufficiale giudiziario consegna o deposita la copia dell'atto da notificare in busta che provvede a sigillare e su cui trascrive il numero cronologico della notificazione, dandone atto nella relazione in calce all'originale e alla copia dell'atto stesso. Sulla busta non sono apposti segni o indicazioni dai quali possa desumersi il contenuto dell'atto. Le disposizioni di cui al terzo comma si applicano anche alle comunicazioni effettuate con biglietto di cancelleria ai sensi degli articoli 133 e 136..

2. Al primo comma dell'articolo 138 del codice di procedura civile, le parole da: può sempre eseguire a destinatario, sono sostituite dalle seguenti: esegue la notificazione di regola mediante consegna della copia nelle mani proprie del destinatario, presso la casa di abitazione oppure, se ciò non è possibile,.

3. Nel quarto comma dell'articolo 139 del codice di procedura civile, la parola: l'originale è sostituita dalle seguenti: una ricevuta.

4. Nell'articolo 140 del codice di procedura civile, dopo le parole: affigge avviso del deposito sono inserite le seguenti: in busta chiusa e sigillata.

5. All'articolo 142 del codice di procedura civile sono apportate le seguenti modificazioni:

   (a) il primo e il secondo comma sono sostituiti dal seguente:
   Salvo quanto disposto nel secondo comma, se il destinatario non ha residenza, dimora o domicilio nello Stato e non vi ha eletto domicilio o costituito un procuratore a norma dell'articolo 77, l'atto è notificato mediante spedizione al destinatario per mezzo della posta con raccomandata e mediante consegna di altra copia al pubblico ministero che ne cura la trasmissione al Ministero degli affari esteri per la consegna alla persona alla quale è diretta.;

   (b) nell'ultimo comma le parole: ai commi precedenti sono sostituite dalle seguenti: al primo comma.

6. Nell'articolo 143, primo comma, del codice di procedura civile, sono soppresse le parole da: , e mediante fino alla fine del periodo.

7. All'articolo 151, primo comma, del codice di procedura civile dopo le parole: maggiore celerità sono aggiunte le seguenti: , di riservatezza o di tutela della dignità.

8. All'articolo 250 del codice di procedura civile dopo il primo comma è aggiunto il seguente: L'intimazione di cui al primo comma, se non è eseguita in mani proprie del destinatario o mediante servizio postale, è effettuata in busta chiusa e sigillata..

9. All'articolo 490, terzo comma, del codice di procedura civile è aggiunto, in fine, il seguente periodo: Nell'avviso è omessa l'indicazione del debitore.

10. All'articolo 570, primo comma, del codice di procedura civile le parole: del debitore, sono soppresse e le parole da: informazioni fino alla fine sono sostituite dalle seguenti: informazioni, anche relative alle generalità del debitore, possono essere fornite dalla cancelleria del tribunale a chiunque vi abbia interesse.

11. All'articolo 14, quarto comma, della legge 24 novembre 1981, n. 689, e successive modificazioni, è aggiunto, in fine, il seguente periodo: - Quando la notificazione non può essere eseguita in mani proprie del destinatario, si osservano le modalità previste dall'articolo 137, terzo comma, del medesimo codice..

12. Dopo l'articolo 15 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è inserito il seguente: Articolo 15-bis. (Notificazioni di atti e documenti, comunicazioni ed avvisi) 1. Alla notificazione di atti e di documenti da parte di organi delle pubbliche amministrazioni a soggetti diversi dagli interessati o da persone da essi delegate, nonché a comunicazioni ed avvisi circa il relativo contenuto, si applicano le disposizioni contenute nell'articolo 137, terzo comma, del codice di procedura civile. Nei biglietti e negli inviti di presentazione sono indicate le informazioni strettamente necessarie a tale fine..

13. All'articolo 148 del codice di procedura penale sono apportate le seguenti modificazioni:

    (a) il comma 3 è sostituito dal seguente: 3. L'atto è notificato per intero, salvo che la legge disponga altrimenti, di regola mediante consegna di copia al destinatario oppure, se ciò non è possibile, alle persone indicate nel presente titolo. Quando la notifica non può essere eseguita in mani proprie del destinatario, l'ufficiale giudiziario o la polizia giudiziaria consegnano la copia dell'atto da notificare, fatta eccezione per il caso di notificazione al difensore o al domiciliatario, dopo averla inserita in busta che provvedono a sigillare trascrivendovi il numero cronologico della notificazione e dandone atto nella relazione in calce all'originale e alla copia dell'atto.;

    (b) dopo il comma 5 è aggiunto il seguente: 5-bis. Le comunicazioni, gli avvisi ed ogni altro biglietto o invito consegnati non in busta chiusa a persona diversa dal destinatario recano le indicazioni strettamente necessarie..

14. All'articolo 157, comma 6, del codice di procedura penale le parole: è scritta all'esterno del plico stesso sono sostituite dalle seguenti: è effettuata nei modi previsti dall'articolo 148, comma 3.

15. All'art. 80 delle disposizioni di attuazione del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271, il comma 1 è sostituito dal seguente: 1. Se la copia del decreto di perquisizione locale è consegnata al portiere o a chi ne fa le veci, si applica la disposizione di cui all'articolo 148, comma 3, del codice..

16. Alla legge 20 novembre 1982, n. 890, sono apportate le seguenti modificazioni:

(a) all'articolo 2, primo comma, è aggiunto, in fine, il seguente periodo: Sulle buste non sono apposti segni o indicazioni dai quali possa desumersi il contenuto dell'atto.;

(b) all'articolo 8, secondo comma, secondo periodo, dopo le parole: - L'agente postale rilascia avviso sono inserite le seguenti: , in busta chiusa, del deposito.

Art. 175. Forze di polizia

1. Il trattamento effettuato per il conferimento delle notizie ed informazioni acquisite nel corso di attività amministrative ai sensi dell'articolo 21, comma 1, della legge 26 marzo 2001, n. 128, e per le connessioni di cui al comma 3 del medesimo articolo è oggetto di comunicazione al Garante ai sensi dell'articolo 39, commi 2 e 3.

2. I dati personali trattati dalle forze di polizia, dagli organi di pubblica sicurezza e dagli altri soggetti di cui all'articolo 53, comma 1, senza l'ausilio di strumenti elettronici anteriormente alla data di entrata in vigore del presente codice, in sede di applicazione del presente codice possono essere ulteriormente trattati se ne è verificata l'esattezza, completezza ed aggiornamento ai sensi dell'articolo 11.

3. L'articolo 10 della legge 1 aprile 1981, n. 121, e successive modificazioni, è sostituito dal seguente: Art. 10 (Controlli) 1. Il controllo sul Centro elaborazione dati è esercitato dal Garante per la protezione dei dati personali, nei modi previsti dalla legge e dai regolamenti.

4. I dati e le informazioni conservati negli archivi del Centro possono essere utilizzati in procedimenti giudiziari o amministrativi soltanto attraverso l'acquisizione delle fonti originarie indicate nel primo comma dell'articolo 7, fermo restando quanto stabilito dall'articolo 240 del codice di procedura penale. Quando nel corso di un procedimento giurisdizionale o amministrativo viene rilevata l'erroneità o l'incompletezza dei dati e delle informazioni, o l'illegittimità del loro trattamento, l'autorità precedente ne dà notizia al Garante per la protezione dei dati personali.

5. La persona alla quale si riferiscono i dati può chiedere all'ufficio di cui alla lettera a) del primo comma dell'articolo 5 la conferma dell'esistenza di dati personali che lo riguardano, la loro comunicazione in forma

intellegibile e, se i dati risultano trattati in violazione di vigenti disposizioni di legge o di regolamento, la loro cancellazione o trasformazione in forma anonima.

6. Esperiti i necessari accertamenti, l'ufficio comunica al richiedente, non oltre trenta giorni dalla richiesta, le determinazioni adottate. L'ufficio può omettere di provvedere sulla richiesta se ciò può pregiudicare azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione della criminalità, dandone informazione al Garante per la protezione dei dati personali.

7. Chiunque viene a conoscenza dell'esistenza di dati personali che lo riguardano, trattati anche in forma non automatizzata in violazione di disposizioni di legge o di regolamento, può chiedere al tribunale del luogo ove risiede il titolare del trattamento di compiere gli accertamenti necessari e di ordinare la rettifica, l'integrazione, la cancellazione o la trasformazione in forma anonima dei dati medesimi..

Art. 176. Soggetti pubblici

1. Nell'articolo 24, comma 3, della legge 7 agosto 1990, n. 241, dopo le parole: mediante strumenti informatici sono inserite le seguenti: , fuori dei casi di accesso a dati personali da parte della persona cui i dati si riferiscono,.

2. Nell'articolo 2 del decreto legislativo 30 marzo 2001, n. 165, in materia di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, dopo il comma 1 è inserito il seguente: 1-bis. I criteri di organizzazione di cui al presente articolo sono attuati nel rispetto della disciplina in materia di trattamento dei dati personali..

3. L'articolo 4, comma 1, del decreto legislativo 12 febbraio1993, n. 39, e successive modificazioni, è sostituito dal seguente: 1. È istituito il Centro nazionale per l'informatica nella pubblica amministrazione, che opera presso la Presidenza del Consiglio dei ministri per l'attuazione delle politiche del Ministro per l'innovazione e le tecnologie, con autonomia tecnica, funzionale, amministrativa, contabile e finanziaria e con indipendenza di giudizio..

4. Al Centro nazionale per l'informatica nella pubblica amministrazione continuano ad applicarsi l'articolo 6 del decreto legislativo 12 febbraio 1993, n. 39, nonché le vigenti modalità di finanziamento nell'ambito dello stato di previsione del Ministero dell'economia e delle finanze.

5. L'articolo 5, comma 1, del decreto legislativo n. 39 del 1993, e successive modificazioni, è sostituito dal seguente: 1. Il Centro nazionale propone al Presidente del Consiglio dei ministri l'adozione di regolamenti concernenti la sua organizzazione, il suo funzionamento, l'amministrazione del personale, l'ordinamento delle carriere, nonché la gestione delle spese nei limiti previsti dal presente decreto..

6. La denominazione: Autorità per l'informatica nella pubblica amministrazione contenuta nella vigente normativa è sostituita dalla seguente: Centro nazionale per l'informatica nella pubblica amministrazione.

Art. 177. Disciplina anagrafica, dello stato civile e delle liste elettorali

1. Il comune può utilizzare gli elenchi di cui all'articolo 34, comma 1, del decreto del Presidente della Repubblica 30 maggio 1989, n. 223, per esclusivo uso di pubblica utilità anche in caso di applicazione della disciplina in materia di comunicazione istituzionale.

2. Il comma 7 dell'articolo 28 della legge 4 maggio 1983, n. 184, e successive modificazioni, è sostituito dal seguente: 7. L'accesso alle informazioni non è consentito nei confronti della madre che abbia dichiarato alla nascita di non volere essere nominata ai sensi dell'articolo 30, comma 1, del decreto del Presidente della Repubblica 3 novembre 2000, n. 396..

3. Il rilascio degli estratti degli atti dello stato civile di cui all'articolo 107 del decreto del Presidente della Repubblica 3 novembre 2000, n. 396 è consentito solo ai soggetti cui l'atto si riferisce, oppure su motivata istanza comprovante l'interesse personale e concreto del richiedente a fini di tutela di una situazione giuridicamente rilevante, ovvero decorsi settanta anni dalla formazione dell'atto.

4. Nel primo comma dell'articolo 5 del decreto del Presidente della Repubblica 20 marzo 1967, n. 223, sono soppresse le lettere d) ed e).

5. Nell'articolo 51 del decreto del Presidente della Repubblica 20 marzo 1967, n. 223, il quinto comma è sostituto dal seguente: Le liste elettorali possono essere rilasciate in copia per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio- assistenziale o per il perseguimento di un interesse collettivo o diffuso..

Art. 178. Disposizioni in materia sanitaria

1. Nell'articolo 27, terzo e quinto comma, della legge 23 dicembre 1978, n. 833, in materia di libretto sanitario personale, dopo le parole: - il Consiglio sanitario nazionale e prima della virgola sono inserite le seguenti: e il Garante per la protezione dei dati personali.

2. All'articolo 5 della legge 5 giugno 1990, n. 135, in materia di AIDS e infezione da HIV, sono apportate le seguenti modifiche:

   (a) il comma 1 è sostituito dal seguente: 1. L'operatore sanitario e ogni altro soggetto che viene a caso di AIDS, ovvero di un caso di infezione da HIV, anche non accompagnato da conoscenza di un stato morboso, è tenuto a prestare la necessaria assistenza e ad adottare ogni misura o accorgimento occorrente per la tutela dei diritti e delle libertà fondamentali dell'interessato, nonché della relativa dignità.;

   (b) nel comma 2, le parole: decreto del Ministro della sanità sono sostituite dalle seguenti: decreto del Ministro della salute, sentito il Garante per la protezione dei dati personali.

3. Nell'articolo 5, comma 3, del decreto legislativo 30 dicembre 1992, n. 539, e successive modificazioni, in materia di medicinali per uso umano, è inserito, infine, il seguente periodo: Decorso tale periodo il farmacista distrugge le ricette con modalità atte ad escludere l'accesso di terzi ai dati in esse contenuti..

4. All'articolo 2, comma 1, del decreto del Ministro della sanità in data 11 febbraio 1997, pubblicato sulla Gazzetta Ufficiale n. 72 del 27 marzo 1997, in materia di importazione di medicinali registrati all'estero, sono soppresse le lettere f) ed h).

5. Nel comma 1, primo periodo, dell'articolo 5-bis del decreto-legge 17 febbraio 1998, n. 23, convertito, con modificazioni, dalla legge 8 aprile 1998, n. 94, le parole da: riguarda anche fino alla fine del periodo sono sostituite dalle seguenti: è acquisito unitamente al consenso relativo al trattamento dei dati personali.

Art. 179. Altre modifiche

1. Nell'articolo 6 della legge 2 aprile 1958, n. 339, sono soppresse le parole: ; mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare e: garantire al lavoratore il rispetto della sua personalità e della sua libertà morale;.

2. Nell'articolo 38, primo comma, della legge 20 maggio 1970, n. 300, sono soppresse le parole: 4, e ,8.

3. Al comma 3 dell'articolo 12 del decreto legislativo 22 maggio 1999, n. 185, in materia di contratti a distanza, sono aggiunte infine le seguenti parole: , ovvero, limitatamente alla violazione di cui all'articolo 10, al Garante per la protezione dei dati personali.

Capo II - Disposizioni transitorie

Art. 180. Misure di sicurezza

1. Le misure minime di sicurezza di cui agli articoli da 33 a 35 e all'allegato B) che non erano previste dal decreto del Presidente della Repubblica 28 luglio 1999, n. 318, sono adottate entro il 31 marzo 2006.

2. Il titolare che alla data di entrata in vigore del presente codice dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle misure minime di cui all'articolo 34 e delle corrispondenti modalità tecniche di cui all'allegato B), descrive le medesime ragioni in un documento a data certa da conservare presso la propria struttura.

3. Nel caso di cui al comma 2, il titolare adotta ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti in modo da evitare, anche sulla base di idonee misure organizzative, logistiche o procedurali, un incremento dei rischi di cui all'articolo 31, adeguando i medesimi strumenti al più tardi entro il 30 giugno 2006.

Art. 181. Altre disposizioni transitorie

1. Per i trattamenti di dati personali iniziati prima del 1 gennaio 2004, in sede di prima applicazione del presente codice:

   (a) l'identificazione con atto di natura regolamentare dei tipi di dati e di operazioni ai sensi degli articoli 20, commi 2 e 3, e 21, comma 2, è effettuata, ove mancante, entro il 28 febbraio 2007;

(b) la determinazione da rendere nota agli interessati ai sensi dell'articolo 26, commi 3, lettera a), e 4, lettera a), è adottata, ove mancante, entro il 30 giugno 2004;

(c) le notificazioni previste dall'articolo 37 sono effettuate entro il 30 aprile 2004;

(d) le comunicazioni previste dall'articolo 39 sono effettuate entro il 30 giugno 2004;

lettera abrogata

(e) l'utilizzazione dei modelli di cui all'articolo 87, comma 2, è obbligatoria a decorrere dal 1 gennaio 2005.

2. Le disposizioni di cui all'articolo 21-bis del decreto del Presidente della Repubblica 30 settembre 1963, n. 1409, introdotto dall'articolo 9 del decreto legislativo 30 luglio 1999, n. 281, restano in vigore fino alla data di entrata in vigore del presente codice.

3. L'individuazione dei trattamenti e dei titolari di cui agli articoli 46 e 53, da riportare nell'allegato C), è effettuata in sede di prima applicazione del presente codice entro il 30 giugno 2004.

4. Il materiale informativo eventualmente trasferito al Garante ai sensi dell'articolo 43, comma 1, della legge 31 dicembre 1996, n. 675, utilizzato per le opportune verifiche, continua ad essere successivamente archiviato o distrutto in base alla normativa vigente.

5. L'omissione delle generalità e degli altri dati identificativi dell'interessato ai sensi dell'articolo 52, comma 4, è effettuata sulle sentenze o decisioni pronunciate o adottate prima dell'entrata in vigore del presente codice solo su diretta richiesta dell'interessato e limitatamente ai documenti pubblicati mediante rete di comunicazione elettronica o sui nuovi prodotti su supporto cartaceo o elettronico. I sistemi informativi utilizzati ai sensi dell'articolo 51, comma 1, sono adeguati alla medesima disposizione entro dodici mesi dalla data di entrata in vigore del presente codice.

6. Le confessioni religiose che, prima dell'adozione del presente codice, abbiano determinato e adottato nell'ambito del rispettivo ordinamento le garanzie di cui all'articolo 26, comma 3, lettera a), possono proseguire l'attività di trattamento nel rispetto delle medesime.

6-bis. Fino alla data in cui divengono efficaci le misure e gli accorgimenti prescritti ai sensi dell'articolo 132, comma 5, per la conservazione del traffico telefonico si osserva il termine di cui all'articolo 4, comma 2, del decreto legislativo 13 maggio 1998, n. 171.

Art. 182. Ufficio del Garante

1. Al fine di assicurare la continuità delle attività istituzionali, in sede di prima applicazione del presente codice e comunque non oltre il 31 marzo 2004, il Garante:
   (a) può individuare i presupposti per l'inquadramento in ruolo, al livello iniziale delle rispettive qualifiche e nei limiti delle disponibilità di organico, del personale appartenente ad amministrazioni pubbliche o ad enti pubblici in servizio presso l'Ufficio del Garante in posizione di fuori ruolo o equiparato alla data di pubblicazione del presente codice;
   (b) può prevedere riserve di posti nei concorsi pubblici, unicamente nel limite del trenta per cento delle disponibilità di organico, per il personale non di ruolo in servizio presso l'Ufficio del Garante che abbia maturato un'esperienza lavorativa presso il Garante di almeno un anno.

Capo III - Abrogazioni

Art. 183. Norme abrogate

1. Dalla data di entrata in vigore del presente codice sono abrogati:
   (a) la legge 31 dicembre 1996, n. 675;
   (b) la legge 3 novembre 2000, n. 325;
   (c) il decreto legislativo 9 maggio 1997, n. 123;
   (d) il decreto legislativo 28 luglio 1997, n. 255;
   (e) l'articolo 1 del decreto legislativo 8 maggio 1998, n. 135;
   (f) il decreto legislativo 13 maggio 1998, n. 171;
   (g) il decreto legislativo 6 novembre 1998, n. 389;
   (h) il decreto legislativo 26 febbraio 1999, n. 51;
   (i) il decreto legislativo 11 maggio 1999, n. 135;

(j) il decreto legislativo 30 luglio 1999, n. 281, ad eccezione degli articoli 8, comma 1, 11 e 12;

(k) il decreto legislativo 30 luglio 1999, n. 282;

(l) il decreto legislativo 28 dicembre 2001, n. 467;

(m) il decreto del Presidente della Repubblica 28 luglio 1999, n. 318.

2. Dalla data di entrata in vigore del presente codice sono abrogati gli articoli 12, 13, 14, 15, 16, 17, 18, 19 e 20 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501.

3. Dalla data di entrata in vigore del presente codice sono o restano, altresì, abrogati:

(a) l'art. 5, comma 9, del decreto del Ministro della sanità 18 maggio 2001, n. 279, in materia di malattie rare;

(b) l'articolo 12 della legge 30 marzo 2001, n. 152;

(c) l'articolo 4, comma 3, della legge 6 marzo 2001, n. 52, in materia di donatori midollo osseo;

(d) l'articolo 16, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, in materia di certificati di assistenza al parto;

(e) l'art. 2, comma 5, del decreto del Ministro della sanità 27 ottobre 2000, n. 380, in materia di flussi informativi sui dimessi dagli istituti di ricovero;

(f) l'articolo 2, comma 5-quater 1, secondo e terzo periodo, del decreto-legge 28 marzo 2000, n. 70, convertito, con modificazioni, dalla legge 26 maggio 2000, n. 137, e successive modificazioni, in materia di banca dati sinistri in ambito assicurativo;

(g) l'articolo 6, comma 4, del decreto legislativo 5 giugno 1998, n. 204, in materia di diffusione di dati a fini di ricerca e collaborazione in campo scientifico e tecnologico;

(h) l'articolo 330-bis del decreto legislativo 16 aprile 1994, n. 297, in materia di diffusione di dati relativi a studenti;

(i) l'articolo 8, quarto comma, e l'articolo 9, quarto comma, della legge 1 aprile 1981, n. 121.

4. Dalla data in cui divengono efficaci le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 118, i termini di conser-

vazione dei dati personali individuati ai sensi dell'articolo 119, eventualmente previsti da norme di legge o di regolamento, si osservano nella misura indicata dal medesimo codice.

Capo IV - Norme finali

Art. 184. Attuazione di direttive europee

1. Le disposizioni del presente codice danno attuazione alla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, e alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002.

2. Quando leggi, regolamenti e altre disposizioni fanno riferimento a disposizioni comprese nella legge 31 dicembre 1996, n. 675, e in altre disposizioni abrogate dal presente codice, il riferimento si intende effettuato alle corrispondenti disposizioni del presente codice secondo la tavola di corrispondenza riportata in allegato.

3. Restano ferme le disposizioni di legge e di regolamento che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali.

Art. 185. Allegazione dei codici di deontologia e di buona condotta

1. L'allegato A) riporta, oltre ai codici di cui all'articolo 12, commi 1 e 4, quelli promossi ai sensi degli articoli 25 e 31 della legge 31 dicembre 1996, n. 675, e già pubblicati nella Gazzetta Ufficiale della Repubblica italiana alla data di emanazione del presente codice.

Art. 186. Entrata in vigore

1. Le disposizioni di cui al presente codice entrano in vigore il 1 gennaio 2004, ad eccezione delle disposizioni di cui agli articoli 156, 176, commi 3, 4, 5 e 6, e 182, che entrano in vigore il giorno successivo alla data di pubblicazione del presente codice. Dalla medesima data si osservano altresì i termini in materia di ricorsi di cui agli articoli 149, comma 8, e 150, comma 2.

Appendice B

Allegato B

Codice in materia di protezione dei dati personali B. Disciplinare tecnico in materia di misure minime di sicurezza (Artt. da 33 a 36 del Codice)

Trattamenti con strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica
1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico

non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza
15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale

dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza
19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. 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 è programmata già al momento dell'ingresso in servizio, nonchè in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in

conformità al codice, all'esterno della struttura del titolare;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari
20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia
25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici
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:
27. 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.
28. 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 dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
29. L'accesso agli archivi contenenti dati sensibili o giudiziari è 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.

Indice analitico