

# Capire la Privacy

## Indice

1	introduzione.....	2
1.1	obiettivi del materiale didattico.....	2
2	cos'è la Privacy .....	2
2.1	il diritto alla protezione dei dati.....	2
2.2	l'oggetto della privacy.....	3
2.3	i reati informatici.....	3
3	il Codice Privacy.....	4
3.1	la struttura e i contenuti.....	4
3.1.1	altre norme: mappa orientativa.....	5
3.2	i principi generali del codice.....	6
3.2.1	i tipi di dato.....	6
3.2.2	i ruoli.....	7
3.2.2.1	l'interessato.....	7
3.2.2.2	i ruoli nell'organizzazione.....	8
3.2.2.3	il Garante.....	9
3.2.3	il trattamento dei dati.....	9
3.2.3.1	il trattamento e i requisiti dei dati.....	10
3.2.3.2	l'utilizzo di strumenti elettronici.....	10
3.2.3.3	misure minime di sicurezza.....	10
3.2.3.4	i soggetti pubblici.....	11
3.2.4	i processi di attuazione.....	11
3.2.4.1	l'informativa e il consenso.....	12
3.2.4.2	nomine e incarichi.....	14
3.2.4.3	DPS.....	15
3.2.5	il caso del Registro Imprese.....	17
3.3	nuove garanzie nel diritto.....	18
4	sintesi dei concetti.....	19
5	conclusioni.....	20
5.1	riepilogo del materiale didattico.....	20

# 1 introduzione

## 1.1 obiettivi del materiale didattico

Gli obiettivi che si pone questa seconda mappa sono così sintetizzabili

- definire il concetto di Privacy, comprendere cosa è oggetto di Privacy e cosa non lo è
- definire gli utilizzi impropri dei dati e i reati connessi
- comprendere i concetti fondamentali legati alla Privacy: il trattamento dei dati, i ruoli e gli incarichi delle persone che hanno a che fare con dati personali, i tipi di dato, i "documenti" previsti e il loro ruolo
- conoscere le caratteristiche principali del Codice Privacy e del contesto normativo in cui il codice si inserisce

Anche in questo modulo cercheremo di andare oltre le semplici definizioni concettuali, con esemplificazioni concrete e facilmente riferibili alla realtà quotidiana.

Particolare rilevanza avrà la trattazione della Privacy in ambito di trattamento elettronico dei dati.

Questo ci consentirà di affrontare il terzo modulo - la Sicurezza Informatica - con alcune conoscenze già affermate e condivise sul trattamento con strumenti elettronici.

## 2 cos'è la Privacy

Per approfondire il tema e i concetti fondamentali della Privacy riprendiamo la definizione già enunciata nel primo modulo:

"Privacy è il diritto alla riservatezza delle informazioni personali e della propria vita privata. Il concetto di privacy si è ampliato nel tempo: all'inizio con privacy si intendeva soprattutto l'azione di impedire che i dati che riguardano la persona siano noti ad altri; nel tempo il concetto si è esteso al diritto di controllare le proprie informazioni personali fino a comprendere l'idea di "sovranità su di sé" e di tutela della propria libertà personale. La Privacy è il riconoscimento di un diritto della persona."

Privacy quindi è anello di congiunzione fra il Diritto e la Persona, in particolar modo per la tutela dei dati che la riguardano.

### 2.1 il diritto alla protezione dei dati

La **Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali** all'Art. 8 sul Diritto al rispetto della vita privata e familiare afferma che: *Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza.*

Il **Codice Privacy** - cioè il decreto 196 / 2003 che analizzeremo in dettaglio - apre con questa definizione :

## *Art. 1. Diritto alla protezione dei dati personali*

### *1. Chiunque ha diritto alla protezione dei dati personali che lo riguardano.*

Una persona fornisce i propri dati personali in innumerevoli occasioni. Le informazioni relative alle persone - **dati personali** - vengono infatti raccolte e utilizzate in molti ambiti della vita quotidiana, quali il lavoro, i servizi per la salute e la famiglia, il tempo libero. I dati personali possono essere raccolti direttamente dalla persona o dalla base di dati esistente e possono essere utilizzati, successivamente, per altri scopi e/o comunicati a terzi.

Come abbiamo considerato nel primo modulo i progressi registrati dall'informatica unitamente alle nuove reti di telecomunicazione consentono ai dati personali di circolare con maggiore facilità. Poiché i dati personali vengono raccolti e scambiati con maggiore frequenza, è necessario regolamentarne il trattamento, la conservazione e il trasferimento.

Vedremo di seguito i principali aspetti normativi e applicativi inerenti al trattamento e protezione dei dati personali.

## **2.2 l'oggetto della privacy**

Premesso che le definizioni sono spesso semplici "chiavi di lettura", per nulla esaustive ma che ci aiutano a capire realtà complesse, possiamo proporre una definizione di Privacy che si raccorda con il contesto digitale attuale e si inserisce in quel "mondo di BIT" di cui abbiamo parlato diffusamente nel modulo uno.

Proprio perché consideriamo la Privacy in relazione al trattamento elettronico dei dati personali e agli strumenti e alle tecniche di Sicurezza Informatica possiamo affermare che:

**PRIVACY è il diritto fondamentale degli individui di poter controllare la raccolta e l'elaborazione dei propri dati personali e di avere la garanzia che le proprie informazioni siano protette da uso non corretto e da improprie diffusioni.**

## **2.3 i reati informatici**

Fra i rischi che incombono sui dati personali vi sono anche interventi illeciti da parte di terzi, normalmente estranei ai flussi ordinari di trattamento. Queste attività sono considerate "reati informatici".

La **frode informatica**, ad esempio, costituisce reato a partire dalla legge n. 547/1993 (art. 10), disciplinata dall'art. 640 ter del c.p.

Il delitto di frode informatica è commesso da "chiunque":

- altera in qualsiasi modo il funzionamento di un sistema informatico o telematico
- **interviene** senza diritto con qualsiasi modalità **su dati, informazioni** o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti

al fine di procurare a sé o ad altri un ingiusto profitto con altrui danno.

Ne consegue che la frode informatica va nella direzione inversa rispetto agli obiettivi di tutela e protezione dei dati, propri della Privacy.

Il Codice della Privacy, infatti, tutela innanzitutto la Riservatezza ma anche la Disponibilità e l'Integrità dei dati. I reati informatici quali il furto e la frode di informazioni digitali possono, al contrario, danneggiare i dati e quindi il Titolare e il Responsabile devono adottare le misure minime di sicurezza atte a prevenire questo tipo di reati, a pena di loro responsabilità anche penali.

### 3 il Codice Privacy

Il Codice Privacy disciplina la protezione dei dati personali stabilendo che qualsiasi trattamento, informatico o cartaceo, di dati personali deve rispettare tale diritto.

Il Decreto legislativo 30 giugno 2003, n. 196 recante il **Codice in materia di protezione dei dati personali** è comunemente chiamato **CODICE PRIVACY**.

Dopo aver affrontato i principi e i concetti principali della Privacy, possiamo più agevolmente fare alcune considerazioni di carattere generale sul Codice per comprenderne:

- la struttura e i contenuti del codice
- il valore e il carattere innovativo dell'attuale normativa sulla privacy
- il rapporto con le altre principali norme

#### 3.1 la struttura e i contenuti

Il Codice Privacy è un **testo unico** ed è entrato in vigore il primo gennaio 2004; abroga e sostituisce la legge del 31 dicembre 1996, n. 675, meglio conosciuta come Legge sulla Privacy.

Il Codice Privacy si pone come il primo modello di legislazione organica e completa, che racchiude in un testo unitario l'intera disciplina della materia considerata.

Più complessivamente il Codice Privacy:

- riordina e razionalizza norme precedenti
- recepisce interpretazioni Garante
- introduce novità e semplificazioni
- recepisce direttiva 2002/58/CE

Il Codice della Privacy ha questa struttura di contenuti

- principi generali protezione dati personali
- regole generali sul trattamento dati personali
- disposizioni su titolari, responsabili, incaricati
- disciplina adempimenti: notifica e autorizzazione Garante, informativa e consenso dell'interessato, ecc.
- disposizioni su misure di sicurezza
- disciplina del Garante

- sanzioni amministrative e penali
- disposizioni transitorie e finali

Completano il testo normativo una serie di allegati:

- allegato A, relativo ai codici di condotta
- allegato B, recante il disciplinare tecnico in materia di misure minime di sicurezza
- allegato C, relativo ai trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia
- la Tavola di corrispondenza dei riferimenti previgenti al Codice in materia di protezione dei dati personali che consente di conoscere, per ciascun articolo del Codice l'eventuale riferimento a norme già esistenti prima dell'entrata in vigore del Codice stesso.

Fra i materiali di approfondimento di questo corso sono disponibili, fra l'altro:

- testo integrale del CODICE PRIVACY
- Allegato B con il disciplinare tecnico
- Tavola di Corrispondenza dei riferimenti previgenti

### 3.1.1 altre norme: mappa orientativa

Il Decreto legislativo n. 196 del 30 giugno 2003, recante il **Codice in materia di protezione dei dati personali** - e comunemente chiamato **CODICE PRIVACY** -, come già accennato precedentemente, raccoglie in modo sistematico e aggiornato le norme e le indicazioni di altri testi legislativi.

Di seguito una mappa orientativa del quadro normativo preesistente, o comunque collegato, al Codice Privacy, che riguarda più da vicino il nostro corso:

- **Legge del 31 dicembre 1996, n. 675** , meglio conosciuta come **Legge sulla Privacy**, che Il Codice Privacy abroga e sostituisce
- **Decreto del Presidente della Repubblica n. 318 del 28 luglio 1999** : regolamento recante norme per l'individuazione delle **misure minime di sicurezza per il trattamento dei dati personali**, a norma dell'articolo 15, comma 2, della legge n. 675 del 31 dicembre 1996
- **Decreto legislativo n. 135 del 11 maggio 1999** : disposizioni integrative della legge 31 dicembre 1996, n. 675, sul **trattamento di dati sensibili da parte dei soggetti pubblici**
- **Decreto del Presidente della Repubblica n. 501 del 31 marzo 1998** : **Regolamento dell'Ufficio del Garante**

Inoltre il Codice si ispira alla **Carta dei diritti fondamentali dell'Unione Europea (2000/C 364/01)**, dove "*l'Unione riconosce i diritti, le libertà ed i principi enunciati*" nel testo della Carta stessa.

### 3.2 i principi generali del codice

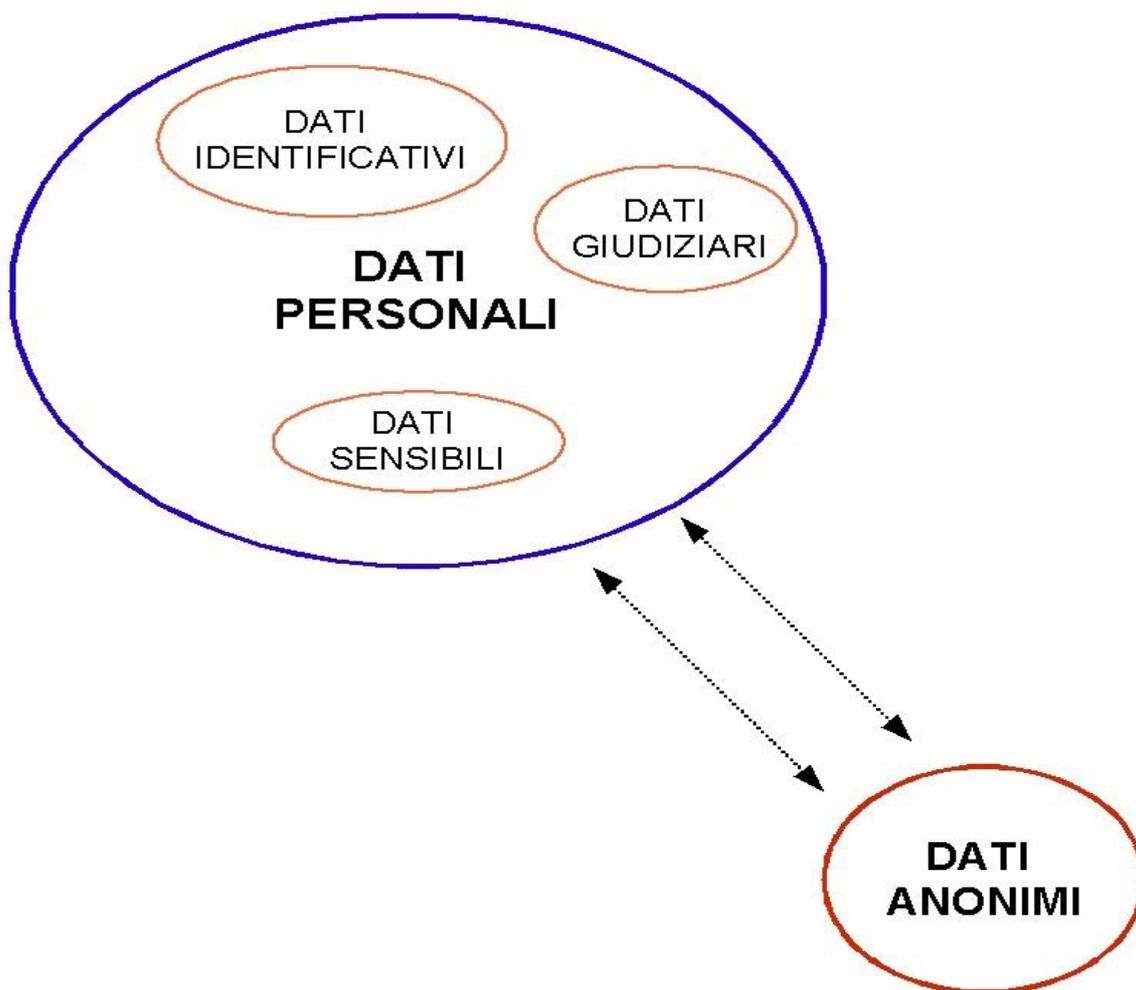
CAPIRE LA PRIVACY è il titolo ed è l'obiettivo principale di questo modulo didattico.

Affrontiamo inizialmente i principi generali e i concetti principali della Privacy, partendo dalle definizioni che ne dà il Decreto Legislativo 30 Giugno 2003, n. 196 - di seguito Codice Privacy - e completandone la descrizione e la lettura critica.

Per le definizioni tratte dal codice si offrono i riferimenti dell'articolo normativo coinvolto.

#### 3.2.1 i tipi di dato

Vi sono **diverse tipologie di dati** cui si fa riferimento sia nella normativa sulla Privacy che nella sua applicazione. Ecco uno schema riassuntivo.



Il Codice Privacy (DL 193/03) definisce i **dati personali** "*qualunque informazione relativa a persona fisica, persona giuridica ente o associazione...*", sia che permettano una identificazione diretta o indiretta del soggetto (art 4, comma 1b).

La normativa entra ancor più in dettaglio e definisce ulteriori tipologie di dati:

- **dati identificativi:** *"i dati personali che permettono l'identificazione diretta dell'interessato"* (art 4 comma 1c);
- **dati sensibili :** i dati inerenti alla sfera religiosa, filosofica, politica o sindacale del soggetto e quelli che possono rivelare il suo stato di salute o la sua vita sessuale (art 4, comma 1d);
- **dati giudiziari :** i dati che possono rivelare informazioni su provvedimenti giudiziari e amministrativi riferiti al soggetto o essere in qualità di imputato o di indagato (art 4 comma 1e).

Il Codice Privacy stabilisce il **diritto di ogni soggetto alla protezione dei propri dati personali** (art 1) e introduce il **principio di necessità** secondo il quale l'utilizzo di tali dati deve essere ridotto al minimo indispensabile (art. 3). In questo modo se ne esclude il trattamento nel momento in cui è possibile perseguire le medesime finalità attraverso l'impiego , *"rispettivamente, di dati anonimi o di opportune modalità, che permettano di identificare l'interessato solo in caso di necessità"* (art 3).

Con il termine **dato anonimo** si definisce il dato che in origine, o a seguito di trattamento , non può essere associato ad uno specifico soggetto o comunque attraverso di esso non è facilmente identificabile (art 4 comma 1n).

Alcune categorie di dati di per sè anonimi, se collegati a dati identificativi dell'interessato, in determinati trattamenti, di fatto perdono l'anonimato e tornano ad essere dati personali (Cfr. schema precedente).

Esempio: i dati di traffico di un numero di telefono cellulare (chiamate, data, ora, numero chiamante o chiamato, durata della conversazione) sono di per sè anonimi finché il numero di telefono non è associato ai dati anagrafici di titolarità del numero di telefono stesso; tale associazione è invece indispensabile e pertanto avviene ad esempio nei trattamenti necessari alle indagini di polizia.

Al contrario questa associazione fra dati anonimi e identificativi del titolare non è necessaria ad esempio nelle elaborazioni contabili del traffico relativo al numero.

### 3.2.2 i ruoli

Nel processo di trattamento dei dati personali sono individuati diversi ruoli, che verranno approfonditi di seguito, e sono:

- l'interessato
- i ruoli specifici dell'organizzazione, quali il Titolare, il Responsabile e gli incaricati
- il Garante

#### 3.2.2.1 l'interessato

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

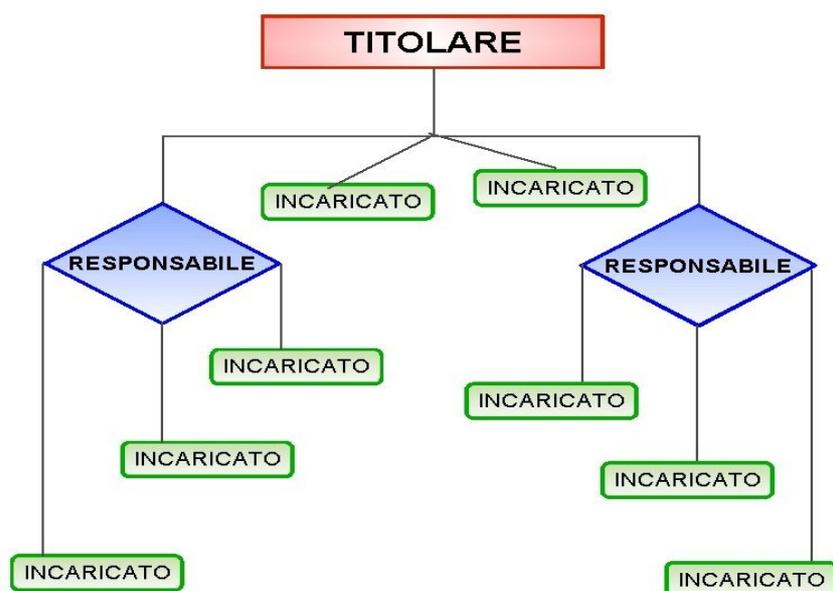
## DIRITTI DELL'INTERESSATO AL TRATTAMENTO DEI DATI PERSONALI

1. di avere la conferma, da parte di enti o persone fisiche, della conoscenza dei propri dati personali
2. di essere informato sulle finalità e modalità del trattamento e se i dati saranno comunicati a terzi
3. di ottenere l'aggiornamento, la rettificazione, ma anche la cancellazione, la trasformazione in forma anonima o il blocco dei dati
4. di opporsi, in tutto o in parte, al trattamento dei propri dati personali

I diritti appena illustrati sono descritti in modo più completo all'art. 7 del Codice Privacy (disponibile fra i materiali di approfondimento di questo corso)

### **3.2.2.2 i ruoli nell'organizzazione**

Nel trattamento dei dati all'interno delle organizzazioni si identificano diversi RUOLI, ciascuno dei quali ha specifici compiti e differenti responsabilità rispetto al processo di trattamento dei dati.



Per **Titolare** si intende *"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, a cui competono le decisioni"* (art 4 comma 1. f) rispetto a:

- le finalità del trattamento dei dati
- le modalità secondo cui devono essere svolte le singole operazioni nel trattamento dei dati
- gli strumenti da utilizzare e le misure di sicurezza da adottare

Il **Responsabile** si identifica con *"la persona fisica, la persona giuridica, la pubblica amministrazione o qualsiasi altro ente, che viene indicato dal Titolare ed è preposto al trattamento dei dati personali"* (art 4 comma 1.g).

Infine gli **incaricati** sono *"le persone autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile"* (art 4 comma 1.h), sono coloro che concretamente nelle loro attività lavorative operano con dati personali.

### **3.2.2.3 il Garante**

L'attività del **Garante**, iniziata nel 1997, pervade ogni ambito in cui vi è la necessità di proteggere dei dati personali. Nello specifico i compiti del Garante sono:

- il **controllo della conformità dei trattamenti di dati personali a leggi e regolamenti** e la segnalazione ai Titolari o ai Responsabili dei trattamenti delle modifiche da adottare per conseguire tale conformità
- l'**esame delle segnalazioni e dei reclami degli interessati**
- la stesura di una **relazione annuale sull'attività svolta e sullo stato di attuazione della legge** e la sua trasmissione al Parlamento e al Governo

### **3.2.3 il trattamento dei dati**

Il Codice Privacy definisce e descrive in modo ampio il significato del concetto **"trattamento dei dati"**( art 4 comma 1a).

Per trattamento dei dati si intende *"qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici..."*, concernenti in termini generali la raccolta, l'utilizzo, il passaggio a terzi, la conservazione e la distruzione di dati.

Nel trattamento si identificano e distinguono diverse "operazioni" che sono:

- **la comunicazione** intesa come il dare conoscenza, o il mettere a disposizione per un'eventuale consultazione, dei dati personali comunicandoli a uno o più soggetti determinati e identificati, diversi da quelli coinvolti direttamente nel processo di trattamento dei dati precedentemente descritti
- **la diffusione** avviene quando i dati personali sono messi a disposizione di qualsiasi soggetto
- **la creazione di una banca dati** cioè l'organizzazione dei dati personali all'interno di una struttura complessa

- **il blocco** sui dati personali in conservazione per il quale non è possibile temporaneamente eseguire ulteriori operazioni

Esempi:

- una richiesta alla CCIAA, da parte di un'impresa, di dati relativi a un'altra impresa costituisce un esempio di comunicazione
- il set di informazioni di un'Impresa messa a disposizione nel Portale delle Imprese in Internet, costituisce un esempio di diffusione perché il dato è a disposizione di chiunque senza riconoscimento

### **3.2.3.1 il trattamento e i requisiti dei dati**

La normativa delinea **le modalità con cui deve avvenire il trattamento dei dati personali** e i **requisiti dei dati** stessi (D.L. 196/2003, art 11).

In sintesi i dati devono:

- **essere raccolti e registrati in modo legittimo e con correttezza** : questo significa attuare tali operazioni esclusivamente per specifici scopi ben esplicitati
- **essere corretti, completi e se necessario aggiornati**; oltre a ciò non devono rivelare informazioni in eccesso, al di fuori di quelle strettamente necessarie agli specifici scopi e non devono nemmeno dare la possibilità di identificare il soggetto oltre il tempo predisposto per raggiungere tali scopi
- i dati personali non trattati secondo le norme vigenti in materia di protezione dei dati personali non possono essere utilizzati.

### **3.2.3.2 l'utilizzo di strumenti elettronici**

Tutte queste operazioni sui dati personali possono avvenire, e di fatto ormai avvengono in massima parte, mediante l'utilizzo di **strumenti elettronici**.

In questo caso subentrano particolari obblighi da seguire e specifiche misure di sicurezza da adottare.

Il Codice Privacy affronta in modo particolare il tema della **Sicurezza dei dati e dei sistemi** al **TITOLO V** e **nell'allegato B)** che rappresenta il **Disciplinare Tecnico** in materie di misure minime di sicurezza.

Di seguito analizziamo sinteticamente le cosiddette "**misure minime**" da adottare nel momento in cui si impiegano, nel trattamento dei dati, degli strumenti elettronici.

### **3.2.3.3 misure minime di sicurezza**

Le **misure minime** sono le misure di natura tecnica, organizzativa e informatica che un titolare adotta per garantire un livello di protezione minimo rispetto ai rischi di cui i dati personali possono essere oggetto.

Se non si stabiliscono e non si adottano misure minime di sicurezza non è consentito raccogliere e trattare dati personali.

*"Il trattamento dei dati personali può essere effettuato tramite l'impiego di strumenti elettronici solo se vengono adottate le seguenti misure minime" (art 34):*

- **autenticazione informatica** : il processo attraverso cui avviene l' identificazione elettronica dell'identità di colui che accede alle postazioni dedicate al trattamento dei dati. Ad esempio l'accesso ai pc può avvenire esclusivamente in seguito all'inserimento di una specifica e personale user-id e password. Oltre a ciò devono essere attive tutte le procedure di gestione e controllo di tale autenticazione.
- **utilizzo sistema di autorizzazione** : sistema per il quale ogni soggetto, impegnato nel trattamento dei dati, non può accedere a tutti i dati indistintamente, ma solo a quelli strettamente necessari per svolgere le proprie attività lavorative. Quindi si deve delineare con precisione quali soggetti possono accedere a quali dati e con quali finalità.
- **adozione di protezioni degli strumenti elettronici e dei dati rispetto a trattamenti illeciti e ad accessi non consentiti** : un esempio può essere l'installazione e il costante aggiornamento dell'anti-virus.
- **creazione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi**
- **tenuta di un aggiornato documento programmatico sulla sicurezza** : è il documento previsto dalla norma in cui vengono esplicitati in modo chiaro sia il trattamento sui dati personali che la descrizione delle misure di sicurezza adottate.

Il **Documento Programmatico sulla Sicurezza** (DPS) verrà descritto più in dettaglio nella sezione dedicata ai "Processi di attuazione".

#### **3.2.3.4 i soggetti pubblici**

La normativa vigente sottolinea come qualunque trattamento di dati personali da parte di **soggetti pubblici** è consentito soltanto (D.L. 196/2003, art 18):

- per lo svolgimento delle **funzioni istituzionali**
- se **autorizzati da espressa disposizione di legge o di regolamento**

Ne consegue che le realtà pubbliche non possono raccogliere dati non previsti dal loro compito istituzionale.

#### **3.2.4 i processi di attuazione**

In questa sezione del corso vengono descritti i processi di attuazione nel trattamento dei dati. I quali sono:

- la realizzazione dell'**Informativa**, come comunicazione del Titolare all'Interessato per esplicitare le modalità e le finalità del trattamento dei dati personali. Da parte sua l'Interessato, attraverso di essa, può esprimere o non esprimere il suo **consenso** al trattamento descritto;
- l'attuazione di **nomine e incarichi**, attraverso i quali scegliere concretamente gli attori nel trattamento dei dati;
- la stesura del **Documento Programmatico sulla Sicurezza (DPS)**, operazione obbligatoria per i privati e le PA che, nel trattamento dei dati, utilizzano strumenti elettronici.

### 3.2.4.1 l'informativa e il consenso

L'**Informativa** è un atto previsto dalla norma ed è la comunicazione attraverso la quale il Titolare informa l'Interessato su come sarà effettuato il trattamento dei dati personali e per quali finalità.

Essa può avvenire sia oralmente che in forma scritta e deve essere fatta all'interessato nel momento della raccolta dei suoi dati personali.

Per capire come si struttura un'informativa, di quali parti è composta e quali sono i suoi macro contenuti, prendiamo quale esempio l'Informativa che ciascun corsista ha sottoscritto per completare l'iscrizione a questo corso e-learning per le CCIAA.

## Corso E-learning

Titolo del Corso .....

CCIAA ..... Cognome ..... Nome .....

### INFORMATIVA ai sensi del D.L. 196/2003 "Codice in materia di Protezione dei Dati Personali"

In relazione alla sua richiesta di frequentare il corso e-learning sopra indicato, ai sensi della normativa in materia di protezione dei dati personali (decreto legislativo 196/03):

- desideriamo ricordarle che anche nell'utilizzo di tale strumento lei è tenuto a rispettare le misure di sicurezza previste in Camera di Commercio
- la informiamo in merito all'utilizzo dei suoi dati personali

#### 1 Fonte dei dati personali

Alcuni suoi dati personali sono raccolti dalla piattaforma di apprendimento online. In particolare il sistema registra gli accessi alle risorse didattiche del corso, la consultazione di pagine di documentazione e filmati, le risposte ai quiz, gli interventi sul forum di discussione.

#### 2 Finalità del trattamento

I dati di accesso e navigazione sono raccolti per l'attività di docenza e tutoring del corso online; con questi dati il tutor è in grado di supportare l'attività formativa di ciascun partecipante e di restituire al corsista i riscontri sull'apprendimento e gli obiettivi formativi raggiunti. L'attività di tutoring consente inoltre, al termine del corso, il rilascio dell'attestato di partecipazione a chi abbia raggiunto gli obiettivi formativi del corso. **A**

#### 3 Modalità di trattamento dei dati

In relazione alle finalità descritte nel precedente paragrafo, il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità sopra evidenziate e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi. **A**

#### 4 Natura del conferimento dei dati e conseguenze di un eventuale rifiuto all'autorizzazione

L'autorizzazione al trattamento dei dati sopra citati è una condizione indispensabile per poter usufruire del corso online. In mancanza di tale autorizzazione l'iscrizione e la frequenza non possono aver luogo. **B**

#### 5 Categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati **C**

I Suoi dati personali potranno essere conosciuti dai dipendenti di InfoCamere appositamente nominati incaricati del trattamento. **D**

#### 6 Diritti dell'Interessato

La informiamo, infine, che la normativa in materia di protezione dei dati personali conferisce agli Interessati la possibilità di esercitare specifici diritti. In particolare, l'Interessato può ottenere:

- a) conferma dell'esistenza o meno di dati che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibili
- b) informazioni circa l'origine dei dati personali, le finalità e le modalità del trattamento nonché la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici
- c) indicazione degli estremi identificativi del Titolare e del Responsabile, nonché dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza;
- d) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché l'aggiornamento, la rettificazione o, quando vi ha interesse, l'integrazione dei dati. **E**

L'Interessato può altresì opporsi, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta. Può inoltre opporsi al trattamento di dati personali ai fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

### 7 Titolare e Responsabili del trattamento

Il Titolare del trattamento dei dati personali di cui alla presente informativa è InfoCamere s.c.p.a.  
Le richieste di cui al precedente paragrafo 6 possono essere presentate a detto Titolare scrivendo al seguente indirizzo: InfoCamere s.c.p.a. Corso Stati Uniti 14 35128 Padova.

### 8 Consenso

F

Io sottoscritto .....

nato a .....

il .....

dipendente della CCIAA di .....

Esprimo  Non esprimo

il consenso al trattamento dei miei dati personali indicati al punto 1 per le finalità indicate.

Data ..... Firma .....

## Analisi Informativa

L'Informativa, sopra riprodotta, riporta al suo interno tutte le informazioni che obbligatoriamente devono essere comunicate all'interessato nel momento in cui si richiede il suo consenso per il trattamento dei dati personali. (art. 13 del D.L. 196/2003)

Nel testo sono stati opportunamente evidenziati la composizione del documento e le varie informazioni contenute.

Le varie parti del documento hanno, nello specifico, questi scopi informativi:

<b>A)</b>	Le finalità e le modalità del trattamento dei dati
<b>B)</b>	La natura obbligatoria o facoltativa del conferimento dei dati
<b>C)</b>	Le conseguenze di un eventuale rifiuto
<b>D)</b>	I soggetti o le categorie di soggetti ai quali tali dati possono essere comunicati
<b>E)</b>	I diritti dell'interessato precedentemente descritti o riportati con maggior completezza nell'art 7 del D.L. 196/2003
<b>F)</b>	Gli estremi identificativi del Titolare

L'obbligatorietà - o meno - del consenso e le eventuali conseguenze del rifiuto del consenso stesso devono essere esplicitati nell'informativa.

L'Interessato prende visione dell'informativa ed eventualmente **esprime / non esprime il proprio consenso** ai trattamenti descritti.

Qualora necessario, solo il consenso da parte dell'interessato rende legittimo il trattamento, che altrimenti non può aver luogo.

Nell' informativa presa come esempio, viene dichiarata la conseguenza del mancato consenso: una persona che chiede l'iscrizione a un corso e-learning ma non manifesta il proprio consenso, non può frequentarlo. (Cfr. punto 4 dell'informativa).

Lo schema, qui sotto riportato, riassume gli aspetti caratterizzanti il complesso rapporto, che si realizza fra Titolare e Interessato nel trattamento dei dati personali.



Quindi il rapporto fra il Titolare e l'Interessato nel trattamento dei dati personali si regola attraverso:

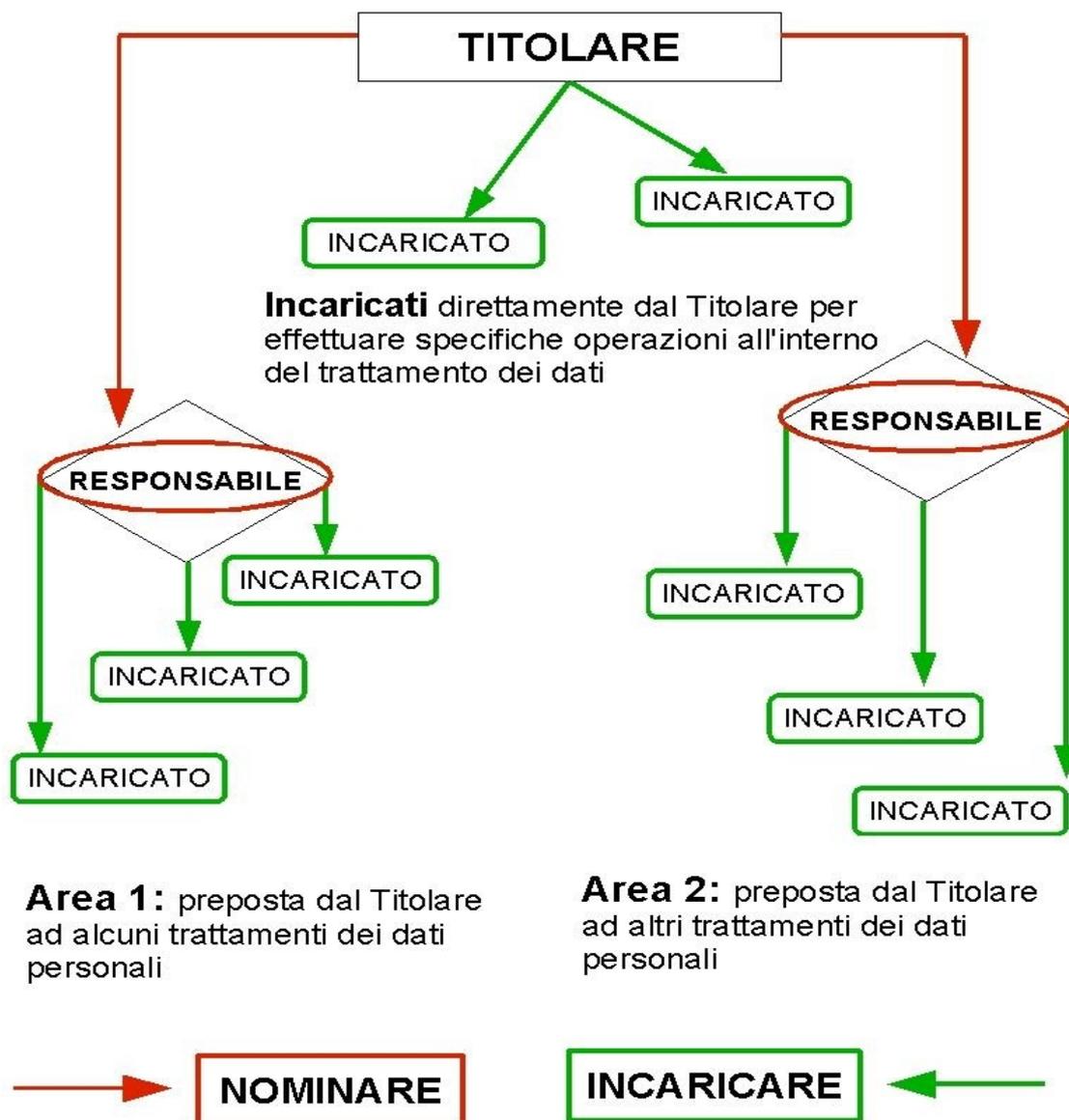
- da una parte, la realizzazione e la consegna dell'Informativa. NB: la consegna può essere effettuata anche dal Responsabile o da un Incaricato;
- dall'altra, la presa visione dell'Informativa e la sottoscrizione o meno del consenso al trattamento.

Oltre a ciò l'Interessato ha la possibilità di esprimere richieste confacenti ai propri diritti, espressi nel Codice della Privacy e riassunti nella specifica sezione di questo corso, dove si delinea tale ruolo. Il Titolare è obbligato, da parte sua, a farsi carico e a rispondere alle suddette richieste.

### **3.2.4.2 nomine e incarichi**

In una precedente sezione del corso sono stati descritti i ruoli che prendono parte al trattamento dei dati.

Nello schema, sotto riprodotto, si vuole sottolineare i legami che intercorrono tra di essi e nello specifico mostrare da chi vengono effettuate le nomine e da chi gli incarichi e chi è l'oggetto di tali processi.



Nello specifico:

- il Titolare ha il potere di **nominare** il Responsabile, il quale può essere sia una persona fisica, giuridica o un Ente;
- gli **incarichi** invece possono essere assegnati sia dal Titolare che dal Responsabile e gli incaricati possono essere solo persone fisiche.

Inoltre il Titolare può nominare più Responsabili, a cui competono spesso differenti trattamenti di dati. Ad esempio può verificarsi la situazione, in cui vi sia un Ente preposto alla raccolta dei dati e un altro invece delegato all'elaborazione di tali dati.

### 3.2.4.3 DPS

Il **Documento Programmatico sulla Sicurezza (DPS)** è innanzitutto un **obbligo di legge**, sia per le organizzazioni pubbliche e private, che utilizzano strumenti elettronici per il trattamento di dati sensibili.

Il DPS costituisce inoltre un'importante **guida per migliorare gli interventi e gli strumenti** adottati per garantire la sicurezza minima nell'effettuare tali complesse e delicate operazioni.

Ogni anno, entro il **31 marzo**, il DPS è redatto o aggiornato.

La tabella seguente sintetizza i temi e gli elementi che devono essere affrontati all'interno del DPS. E' possibile conoscere una descrizione più dettagliata e completa consultando l'Allegato B del DL 196/2003, regola 19.

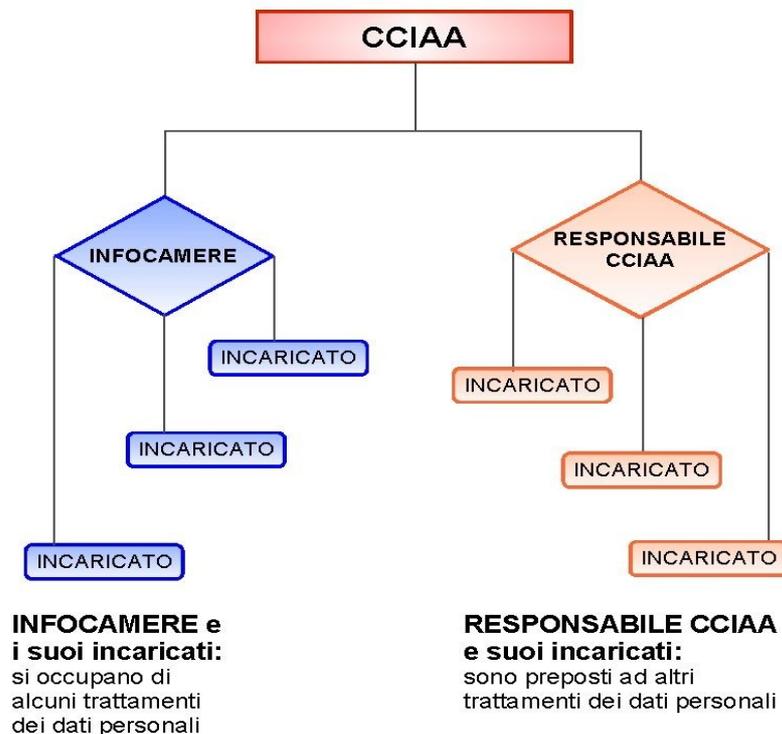
TEMI DA TRATTARE NEL DPS	DESCRIZIONE
ELENCO DEI TRATTAMENTI DI DATI PERSONALI	<p>Si devono riportare dettagliatamente i seguenti aspetti:</p> <ul style="list-style-type: none"> <li>● i trattamenti effettuati</li> <li>● la natura dei dati raccolti, registrati e conservati</li> <li>● le operazioni che ogni struttura (ufficio, area...) interna ed esterna deve svolgere e con quali finalità</li> <li>● gli strumenti elettronici utilizzati</li> </ul>
COMPITI E RESPONSABILITA'	<p>Si deve descrivere l'organizzazione che è stata data alla struttura di riferimento, specificando i singoli compiti e le specifiche responsabilità, derivanti dal diverso trattamento dei dati effettuato. Queste precise indicazioni possono essere riportate, per una miglior presa visione da parte di tutti, in documenti interni, quali circolari, ordini di servizio, ecc.</p>
ANALISI RISCHI DEI DATI	<p>Si deve analizzare i maggiori rischi a cui sono soggetti i dati, precisando le eventuali conseguenze connesse agli strumenti elettronici impiegati e allo specifico contesto fisico-ambientale presente nella struttura di riferimento.</p>
MISURE IN ESSERE E DA ADOTTARE	<p>Si deve descrivere gli interventi tecnici, organizzativi e informatici, che devono essere attuati per far fronte ai rischi individuati. Oltre a ciò devono essere indicate le necessarie verifiche nel tempo per garantire la reale efficacia degli interventi e degli strumenti adottati.</p>

RIPRISTINO DATI	Si devono individuare i criteri e le modalità, attraverso le quali è possibile realizzare il ripristino dei dati, nel momento in cui dovessero verificarsi eccezionali eventi di danneggiamento dei dati e di inaffidabilità degli strumenti e delle procedure utilizzate.
INTERVENTI FORMATIVI	Si devono riportare le informazioni rispetto agli interventi formativi, che si prevede di attuare.
TRATTAMENTI AFFIDATI ALL'ESTERNO	Si deve analizzare le attività affidate a terzi che comportano il trattamento di dati, per garantire una concreta protezione di questi ultimi.

### 3.2.5 il caso del Registro Imprese

Il caso del Registro Imprese può essere esemplificativo di quanto descritto, in termini di trattamento dei dati, ruoli e processi di attuazione.

Nello schema di seguito riportato i termini generali di *Titolare*, *Responsabile* e *Incaricato*, nonché i processi di *nomina* e di *incarico* assumono un'identità o un significato concreto, poiché effettivamente individuati all'interno della realtà in esame.



Nel caso del Registro Imprese, infatti, il Titolare, cioè colui che detiene l'effettivo potere decisionale rispetto alle finalità, alle modalità e agli strumenti del trattamento dei dati personali in essere, è la singola Camera di Commercio.

Ognuna di esse, nell'esplicazione del proprio ruolo, ha nominato poi specifici Responsabili a seconda dei diversi trattamenti da effettuare. Quindi ogni CCIAA ha nominato:

- InfoCamere come Responsabile della conservazione e gestione dei dati del Registro Imprese attraverso strumenti elettronici
- una o più persone fisiche, suoi dipendenti, come Responsabili all'interno della propria organizzazione di altri tipi di trattamento (es. raccolta, diffusione dei dati...).

Per quanto riguarda la nomina degli incaricati ai trattamenti:

- InfoCamere ha nominato suoi dipendenti come incaricati ai trattamenti di cui è responsabile
- la CCIAA stessa ha incaricato suoi dipendenti di effettuare i trattamenti non delegati a InfoCamere

### **3.3 nuove garanzie nel diritto**

Il Codice Privacy risponde all'esigenza di una moderna e aggiornata tutela dei diritti fondamentali della persona e attraverso una serie di **elementi innovativi** pone **nuove garanzie nel diritto**.

[ 1 ]

Il Codice riconosce il **diritto alla protezione dei dati personali**, quale fondamentale attribuzione nuova e autonoma della persona, **parallela al più generale diritto alla riservatezza**.

In questo il Codice si ispira alla Carta dei diritti fondamentali dell'Unione europea, che opera una distinzione tra il tradizionale "rispetto della vita privata e della vita familiare" (art. 7) - che costituisce l'essenza della privacy - e il diritto alla protezione dei dati personali (art. 8).

L'articolo 7 della Carta europea stabilisce **la tutela della riservatezza** quale potere giuridico, che spetta ad ogni persona, che si esaurisce sostanzialmente nell'escludere dalla propria vita privata le interferenze altrui

L'articolo 8 invece afferma il diritto alla **protezione dei dati**, che spetta ad ogni persona e si concretizza nei poteri di intervento di ogni soggetto nei confronti di chiunque gestisca informazioni personali aventi un impatto sociale.

Potremmo dire, con altre parole, che il rispetto della riservatezza è una formula di tutela statica, mentre la protezione dei dati delinea una tutela dinamica che il soggetto stesso può attuare per controllare la circolazione dei dati personali e la loro proiezione nei vari circuiti sociali, economici culturali etc.

In tal modo le regole introdotte costituiscono il punto di equilibrio, individuato dal legislatore, tra l'interesse individuale al controllo dei dati e l'interesse collettivo alla circolazione delle informazioni.

[ 2 ]

Un ulteriore profilo di garanzia si rinviene nella **introduzione del principio di necessità** : i sistemi informativi devono essere predisposti in modo da assicurare che i dati personali o identificativi siano utilizzati solo se indispensabili per il raggiungimento delle finalità

consentite; i dati non devono essere utilizzati invece quando i medesimi obiettivi possono essere raggiunti mediante l'uso dei dati anonimi. Il principio di necessità integra e completa quello di pertinenza e non eccedenza dei dati trattati.

[ 3 ]

Un'altra misura di garanzia rivolta alla protezione dei dati personali è introdotta con l'articolo 11 del Codice laddove la norma dispone che **i dati personali devono essere trattati in modo lecito e secondo correttezza**, raccolti e registrati per scopi determinati, espliciti e legittimi e utilizzati in termini compatibili con tali scopi. A garantire e favorire questi requisiti, la norma configura una misura inibitoria che **invalida un trattamento non conforme**, in quanto i dati personali trattati in violazione di tale disciplina non possono essere utilizzati. Viene a crearsi la categoria giuridica della **inutilizzabilità** dei dati personali nei casi di trattamenti anomali, con l'effetto che il trattamento irregolare non può avere effetti giuridici.

[ 4 ]

In ambito europeo si segnala una sempre maggiore sensibilità al problema della sicurezza informatica.

In sintonia con tali orientamenti, il Codice elabora, nel **Titolo V**, un'efficiente serie di **regole concernenti le misure di sicurezza dei dati e dei sistemi**, con particolare riguardo alle misure minime di sicurezza e alle modalità inerenti sia i trattamenti con strumenti elettronici, sia quelli senza l'ausilio di tali strumenti.

[ 5 ]

Il nuovo Codice ha ampliato notevolmente il nucleo delle regole inerenti ai trattamenti dei dati in ambito pubblico; questo consolida la tutela dei diritti dei cittadini nei confronti dei corpi amministrativi che procedono a trattamenti di dati personali.

Agli articoli 18-22, il Codice :

- definisce i principi generali in base ai quali i soggetti pubblici sono autorizzati a trattare i dati personali e, in particolare quelli sensibili, con specifiche cautele e criteri rigorosi
- individua alcune rilevanti finalità di interesse pubblico per il cui perseguimento è consentito tale trattamento, nonché le operazioni eseguibili e i tipi di dati che possono essere trattati

E' consentito il trattamento dei dati da parte di soggetti pubblici, solo se autorizzato da disposizioni di legge, nelle quali siano specificate, tra l'altro, le rilevanti finalità di interesse pubblico. Ma dove manchi tale esplicita regola, il Garante può determinare, su richiesta dei soggetti pubblici, quelle specifiche attività di interesse pubblico, che valgono ad autorizzare i trattamenti. Viene quindi attribuito al Garante un potere sostitutivo delle norme mancanti.

## 4 sintesi dei concetti

Riprendiamo qui alcuni concetti fondamentali sulla Privacy, in modo da tracciarne un quadro integrato e di facile comprensione.

Come affermato in precedenza, il trattamento dei dati personali è consentito dalla presa visione dell'Informativa e dall'eventuale consenso dell'Interessato. Attraverso l'Informativa l'Interessato deve conoscere le finalità del trattamento e le modalità in cui viene espletato. Deve, inoltre, essere informato su chi tratta i suoi dati, per poter esercitare eventualmente i propri diritti nei confronti del Titolare/Responsabile.

Il Titolare e il Responsabile, da parte loro, devono trattare con correttezza i dati forniti dall'Interessato attraverso anche l'attuazione di misure di sicurezza, al fine di proteggerli da possibili utilizzi fraudolenti, dal danneggiamento casuale o voluto e da ogni altro tipo di rischio significativo.

In poche parole i dati personali, sensibili, giudiziari dell'Interessato devono essere trattati con trasparenza, correttezza e con una 'buona dose' di misure di sicurezza, atte a proteggerli, in relazione alla loro criticità e ai rischi effettivi analizzati.

Quindi l'obiettivo di tutelare la Privacy, nella realtà attuale connessa sempre di più con 'dati' in formato digitale, viene raggiunto anche con un buon utilizzo della Sicurezza Informatica.

Per garantire un grado minimo di sicurezza sono necessari:

- una buona organizzazione in termini procedurali e tecnici nel trattamento dei dati (stesura e aggiornamento DPS, attribuzione dei ruoli...)
- una corretta analisi dei rischi che incombono sui dati
- opportune contromisure per ridurre i rischi riscontrati

Naturalmente l'ambito generale delle misure di Sicurezza è più ampio di quello utilizzato per la Privacy e a volte va addirittura in senso contrario. Un esempio importante sono le misure di sicurezza che invadono più o meno vistosamente la privacy per proteggere altre necessità 'sociali' (e di riflesso anche dell'individuo), quali la sicurezza contro atti di terrorismo o della criminalità organizzata (telecamere, restrizioni di bagaglio o perquisizioni agli aeroporti, intercettazioni ...etc...).

Si può dire che la Sicurezza talora limita certe libertà individuali a garanzia di quelle 'sociali'.

La Privacy, invece, è rivolta direttamente ed esclusivamente alla protezione della sfera individuale di tutti e non toglie 'libertà' a nessuno... se non quella di 'trattare' impropriamente i dati di altri.

## **5 conclusioni**

### ***5.1 riepilogo del materiale didattico***

In questa mappa abbiamo affrontato questi argomenti:

- il concetto di Privacy per comprendere cosa è oggetto di Privacy e cosa non lo è
- definizione degli utilizzi impropri dei dati e i reati connessi
- le caratteristiche principali del Codice Privacy e i suoi aspetti innovativi, un breve

riferimento al contesto normativo in cui il codice si inserisce

- i concetti fondamentali legati alla Privacy: il trattamento dei dati, i ruoli e gli incarichi delle persone che hanno a che fare con dati personali, i tipi di dato, i "documenti" previsti e il loro ruolo