

Privacy e statistica ufficiale

Maria Rosaria Simeone

Dirigente tecnologo – Istat

Direzione Generale

Trento, 14 settembre 2017

L'ufficio di statistica del Sistan. I diversi ruoli

1. Il Comune è «**Titolare**» di indagini statistiche
 - di interesse nazionale (previste nel Programma statistico nazionale)
 - di interesse dell'amministrazione d'appartenenza
2. Il Comune è «**Organo di rilevazione intermedia**» nelle indagini Istat
3. Il Comune è coinvolto in rilevazioni statistiche come «**rispondente**»

Per la corretta gestione e conservazione dei dati è, pertanto, necessario individuare la «**veste**» in cui l'US è di volta in volta chiamato a operare.

Quadro normativo generale

- ❑ **Codice in materia di protezione dei dati personali** – d.lgs. 196/2003, di seguito **Codice**.
- ❑ **Codice di deontologia e buona condotta per il Sistan**, di seguito **Codice deontologico** (*allegato A3 al Codice*)
- ❑ **Decreto legislativo 6.9.1989, n. 322** (*in particolare art. 6-bis*)

(segue) **Quadro normativo generale**

- ❑ **Regolamento (UE) n. 2016/679 del 27 aprile 2016, sulla protezione dei dati (da applicare a decorrere da 25 maggio 2018).**

- ❑ **Disegno di legge n. 4620 (Camera dei deputati) Approvato dal Senato il 2 agosto 2017 - art. 13.**
Il Governo è delegato ad adottare, entro sei mesi dalla data di entrata in vigore della legge, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) n. 2016/679.

(segue) **Quadro normativo generale**

Principi e criteri direttivi della delega:

- a) abrogare le disposizioni del d. lgs. n. 196/2003, non compatibili con le disposizioni del reg. (UE) 2016/679;
- b) modificare il d. lgs. n. 196/2003 laddove necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel reg. (UE) 2016/679;
- c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni del reg. (UE) 2016/679;
- d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi del Garante per la protezione dei dati personali
- e) adeguare il sistema sanzionatorio vigente alle disposizioni del reg. (UE) 2016/679

Definizioni essenziali

TRATTAMENTO: qualunque operazione concernente raccolta, registrazione, elaborazione, cancellazione, distruzione ecc. di dati.

DATO PERSONALE : qualunque informazione riferita a persona fisica (*interessato*) identificata o identificabile* anche indirettamente (documento, immagine, suono, ecc).

Sono quindi dati personali anche i dati sottoposti a pseudonimizzazione** , in quanto esiste comunque la possibilità di attribuirli a una determinata persona fisica mediante l'utilizzo di ulteriori informazioni.

* (Il Codice deontologico definisce identificabile una persona quando con l'impiego di mezzi ragionevoli (tra cui le tecnologie disponibili, i costi e il tempo necessario per l'identificazione) è significativamente probabile stabilire un'associazione tra la combinazione delle modalità delle variabili relative ad una persona e i dati identificativi della medesima.

** (In base al Reg. UE n. 2016/679 per «pseudonimizzazione» si intende «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile)

Definizioni essenziali

DATO ANONIMO: dato che in origine o a seguito di trattamento non è in alcun modo, neanche indirettamente, associabile ad una persona fisica.

La disciplina in materia di dati personali non si applica alle informazioni anonime.

(segue) **Definizioni essenziali**

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;

DATI GIUDIZIARI *: i dati personali idonei a rivelare provvedimenti iscritti nel casellario giudiziario (provvedimenti giudiziari concernenti le pene, le misure alternative alla detenzione, le sanzioni...) e nell'anagrafe delle sanzioni amministrative dipendenti da reato, o la qualità di imputato o di indagato;

*Nel Regolamento (UE) n. 2016/679 si parla «di categorie particolari di dati personali»

(segue) **Definizioni essenziali**

COMUNICAZIONE: dare conoscenza dei dati a soggetti determinati.

DIFFUSIONE: dare conoscenza dei dati a soggetti indeterminati.

I soggetti coinvolti nel trattamento

Titolare (art. 4, comma 1, lett. *f*), d.lgs. n. 196/2003)

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 ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza (**Nel caso di una pubblica amministrazione o altro ente, il titolare è l'entità nel suo complesso o l'unità o organismo periferico con potere decisionale autonomo su finalità e modalità del trattamento**)

Responsabile (art. 4, comma 1, lett. *g*), d.lgs. n. 196/2003)

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali

Incaricato (art. 4, comma 1, lett. *h*), d.lgs. n. 196/2003)

La persona autorizzata per iscritto a compiere determinate operazioni sui dati personali dal titolare o dal responsabile ed operante sotto la diretta autorità di questi ultimi.

I soggetti coinvolti nel trattamento

«Responsabile della protezione dei dati personali» (- DPO)

Figura di rilievo prevista come obbligatoria dal reg. (UE) n. 2016/679 per le Pubbliche amministrazioni

L'articolo 39 del Regolamento specifica nel dettaglio quali sono i compiti minimi del DPO:

- informare e fornire consulenza al titolare e al responsabile del trattamento in merito agli obblighi in materia di protezione dati;
- sorvegliare sull'osservanza del Regolamento;
- fornire, su richiesta, pareri in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;
- cooperare con il Garante privacy e fungere da punto di contatto per tutte le questioni connesse al trattamento

Attenzione: nomina del DPO adempimento prioritario per le PA, auspicabile entro settembre 2017, per partire poi subito dopo con la predisposizione del Registro dei trattamenti

Compiti del Titolare - art. 28 del Codice

IL TITOLARE deve :

Verificare

- a) la sussistenza dei *presupposti normativi* del trattamento ossia il collegamento alle proprie funzioni istituzionali per i dati comuni e le ulteriori condizioni previste dal Codice per i dati sensibili (**V. slides segg.**);
- b) il rispetto dei *principi di cui agli artt. 11 e 22* del Codice

Garantire all'interessato l'esercizio dei diritti di cui all'art. 7 predisponendo misure volte ad agevolare l'accesso e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici preposti alle relazioni con il pubblico.

Assicurarsi che sia resa idonea informativa all'interessato ai sensi dell'art. 13 del Codice.

Compiti del Titolare - art. 28 del Codice

IL TITOLARE deve :

Notificare al Garante i trattamenti rientranti nella previsione dell'art. 37 del Codice (**adempimento da effettuare una tantum**)

Designare i responsabili del trattamento (interni o esterni, ad es. presso gli organi di rilevazione), delimitarne compiti e responsabilità e vigilare sul loro operato;

Definire “la politica di sicurezza” dei dati personali (non è più obbligatoria l'adozione del “*Documento programmatico sulla sicurezza*”)

Compiti del Titolare - art. 28 del Codice

L'art. 30 del Regolamento Europeo 2016/679 dispone che:

Ogni **Titolare** del trattamento tenga un **registro delle attività di trattamento** contenete le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e del responsabile della protezione dei dati; b) le finalità del trattamento; c) una descrizione delle categorie di interessati e di dati personali; d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati; e) i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale; f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Compiti del responsabile - art. 29 del Codice

IL RESPONSABILE, attenendosi alle istruzioni impartite dal Titolare, deve:

Progettare il trattamento in modo da assicurarne la conformità alle norme;

Designare quali incaricati del trattamento tutte le persone, interne o esterne, che collaborano alle attività affidate dal titolare, impartendo loro istruzioni scritte dirette a garantire il corretto svolgimento delle attività, la protezione dei dati trattati e la tutela del segreto statistico (in particolare sono incaricati del trattamento i rilevatori impegnati nell'indagine, ai quali vanno impartite istruzioni dirette a garantire la corretta esecuzione dell'indagine, la protezione dei dati trattati, con particolare riguardo all'art. 10 del *Codice deontologico*, e il segreto statistico);

Curare gli adempimenti necessari a garantire che sia resa idonea informativa agli interessati;

Adottare, nell'ambito della “*politica di sicurezza*” definita dal Titolare, ogni misura idonea ad evitare accessi non autorizzati, trattamenti non consentiti o non conformi alle finalità della raccolta, perdita o distruzione, anche accidentale, dei dati (artt. 31 e seguenti Codice)

Estrarre e comunicare all'interessato, anche attraverso propri incaricati, i dati richiesti nell'esercizio dei diritti di cui all'art. 7 del Codice.

Compiti del responsabile - art. 29 del Codice

L'art. 30 del Regolamento Europeo 2016/679 dispone che ogni **Responsabile** del trattamento tenga **un registro** di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento; b) le categorie dei trattamenti effettuati per conto di ogni titolare; c) i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale; d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Attenzione: Le disposizioni attuative/interpretative dovranno confermare se (come sembra) questo adempimento gravi solo sui responsabili «esterni» (es. responsabile dell'ufficio di statistica che opera per conto dell'Istat nella conduzione delle rilevazioni)

Compiti degli incaricati del trattamento

(art. 30 del Codice)

- “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.”

Presupposti che rendono lecito il trattamento

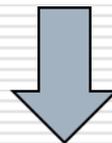
OCCORRE DISTINGUERE TRA

- dati personali comuni (*diversi da quelli sensibili e giudiziari*)
- dati personali sensibili e giudiziari

Presupposti e limiti del trattamento

DATI PERSONALI COMUNI

I soggetti SISTAN



possono TRATTARE lecitamente i dati personali *necessari** al perseguimento degli scopi statistici previsti dal 322/1989 o da altra legge (v. art. 6 bis del d.lgs. n. 322/1989).

(*il principio di necessità impone di *verificare preliminarmente che non sia possibile raggiungere le medesime finalità con l'impiego di dati anonimi* - art. 6-bis del d.lgs. n. 322/1989. Il Principio è ulteriormente rafforzato dal reg. UE 6789/2016)

Presupposti e limiti del trattamento

DATI SENSIBILI e GIUDIZIARI

I soggetti **pubblici** del Sistan possono trattare lecitamente dati sensibili e giudiziari in base all'art. 98, lett. b) del *Codice che qualifica l'attività statistica da essi svolta "di rilevante interesse pubblico"*)

E' però richiesto che:

un **atto regolamentare**

oppure

il **Programma statistico nazionale ***

specificchino

a) i tipi di dati da trattare;

b) le rilevazioni per le quali i dati sono trattati;

c) le modalità del trattamento.

**(E' l'art. 4-bis del Codice deontologico a stabilire che il P.S.N. indichi i dati sensibili e giudiziari oggetto di trattamento, le rilevazioni per le quali gli stessi sono trattati e le modalità del trattamento)*

Principi applicabili al trattamento di dati sensibili e giudiziari

**Art. 22 del Codice
(omissis)**

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.

Progettare la privacy

Il «**Progetto di protezione dei dati**» impone **scelte** preventive in termini di priorità e di bilanciamento tra costi e rischi per i dati personali, tenendo conto della specifica realtà, anche culturale, delle risorse disponibili e degli investimenti possibili.

Tali scelte devono essere **documentate**, anche nell'ottica della «**dimostrabilità**» della conformità delle operazioni di trattamento al nuovo Regolamento.

Ciò consente di ridurre i rischi del trattamento e l'impatto sui diritti degli interessati, ma anche di rafforzare il livello di affidabilità del Titolare

Progettare la privacy

Tale approccio è il cardine del reg. (UE) n. 679/2016

L'art. 25 introduce i principi di «*privacy by design*» e «*privacy by default*»:

- il principio di *privacy by design* (protezione dei dati fin dalla progettazione) impone una valutazione del rischio al momento della progettazione, quindi prima che il trattamento inizi;
- il principio di *privacy by default* (protezione per impostazione predefinita) stabilisce che per impostazione predefinita il Titolare dovrebbe trattare i dati personali solo nella misura necessaria per le finalità previste e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il trattamento di dati in modo da garantire la non eccessività dei dati raccolti. Ciò implica, in altre parole, l'utilizzo di prodotti, servizi e applicazioni concepiti, sin dall'origine, per consentire la minimizzazione dei dati personali e la pseudonimizzazione degli stessi.

Progettare la privacy

Per i trattamenti che presentano un elevato rischio per i diritti e le libertà delle persone, in particolare quando è previsto «l'uso di nuove tecnologie» il Titolare, prima di avviare il trattamento

1. effettua una valutazione di impatto, consultando il Garante laddove necessario.

La **valutazione d'impatto** comprende:

- la descrizione dei trattamenti previsti e loro finalità;
- la valutazione della necessità e proporzionalità dei dati (minimizzazione dei dati personali);
- l'analisi dei rischi per i diritti e le libertà degli interessati;
- l'adozione di misure di sicurezza e garanzie adeguate ai rischi;

2. pone in essere periodicamente procedure di *testing*, verifica e valutazione dell'efficacia complessiva delle misure adottate.

(Un elenco dei trattamenti da sottoporre a Valutazione d'impatto sarà predisposto dal Garante- v.art. 35):

Progettare la privacy

In sostanza, mentre l'approccio della direttiva europea 46/95 era essenzialmente riparatorio, quello del Regolamento si fonda su una tutela preventiva che utilizza gli strumenti della valutazione d'impatto e della protezione fin dalla **progettazione e per impostazione predefinita**. La tutela è anticipata ad un momento anteriore al trattamento.

Tale diversa prospettiva (dalla riparazione dell'illecito alla prevenzione del danno) si riflette anche sulle responsabilità del titolare: non una elencazione dettagliata delle attività da porre in essere ma l'obbligo di valutare preventivamente l'effettiva attitudine al danno di ogni trattamento.

Progettare la privacy in ambito Sistan

Quali dati, da quali fonti?

1. Valutare la necessità e proporzionalità dei dati da trattare in relazione alle finalità perseguite
2. Individuare la fonte legittima dei dati

La raccolta dei dati - regole

Gli uffici di statistica possono raccogliere i dati:

1. presso l'interessato (imprese, istituzioni, famiglie, persone fisiche)

■ direttamente

■ tramite soggetti terzi (pubblici - cd. *organi intermedi di rilevazione* - o privati)

2. presso terzi che li abbiano già raccolti per proprie finalità istituzionali
(*archivi amministrativi*)*

A) per l'attuazione del PSN (*art. 6 comma 1, lett. b del 322*)

B) nei casi previsti da norme legge o di regolamento

C) in tutti i casi diversi da A) e B) se il detentore dei dati è un soggetto pubblico, dandone comunicazione preventiva al Garante per la protezione dei dati personali ai sensi degli artt. 19 e 39, comma 2, del Codice (*comunicazione al Garante e, decorsi 45 giorni senza rilievi, formazione del silenzio - assenso*).

***N.B.** Se i detentori dei dati amministrativi sono soggetti Sistan
l'accesso deve avvenire per il tramite del rispettivo ufficio di statistica

(segue) La raccolta dei dati - regole

■ Se i dati amministrativi sono in possesso della propria amministrazione, l'ufficio di statistica:



può chiederne l'accesso per finalità statistiche (unica eccezione: i dati coperti da segreto in base alla legge o che l'amministrazione ritenga di assoggettare a vincolo di riservatezza (commi 3 e 5 dell'art. 6 del 322)

(segue) La raccolta dei dati - regole

- **In virtù di una espressa previsione normativa**
(art. 8 della legge n. 681/96)

ISTAT

ha accesso a tutti gli archivi di enti pubblici o soggetti a controllo pubblico, anche al di fuori del PSN

(segue) La raccolta dei dati - regole

E' consentita la comunicazione tra gli uffici di statistica del Sistan dei microdati raccolti da ciascun ufficio nell'ambito di proprie rilevazioni statistiche (***interscambio di microdati***).

Limiti e modalità di tale circolazione sono fissati:

- nell'art. 8 del Codice deontologico;
- nella Direttiva del COMSTAT n. 9 del 20.4.2004 (G.U. 23.12.2004).

La raccolta dei dati - Direttiva Comstat n. 9/2004

Direttiva Comstat n. 9/2004 I criteri per l'interscambio dei dati tra uffici di statistica sono diversi a seconda che i dati richiesti servano per l'attuazione del PSN o per soddisfare esigenze conoscitive al di fuori del PSN.

In concreto, l'ente o ufficio di statistica:

- se riceve una richiesta di dati per il PSN deve limitarsi a verificarne la conformità a quanto previsto nel Programma;
- se riceve una richiesta per trattamenti al di fuori del PSN deve valutarne la pertinenza e non eccedenza rispetto alle finalità statistiche dichiarate.

(segue) La raccolta dei dati - Direttiva Comstat n. 9/2004

Ciò in quanto il PSN:

- illustra le finalità perseguite e le garanzie previste a tutela dei diritti dell'interessato;
- indica i dati sensibili, le rilevazioni per le quali essi sono trattati e le modalità del trattamento;
- è adottato sentito il Garante per la protezione dei dati personali.

I diritti dell'interessato

- ✓ **Informativa**
- ✓ **Esercizio dei diritti di cui all'art. 7 del Codice**

I diritti dell'interessato

L'informativa

- oltre alle informazioni di cui all'art. 13 del Codice i soggetti Sistan avvertono l'interessato che i suoi dati saranno utilizzati anche per altri *trattamenti all'interno del Sistan*;
- se i dati sono raccolti presso terzi (da archivi), l'informativa, se eccessivamente onerosa, si considera resa se il trattamento è incluso nel PSN o è oggetto di pubblicità nelle forme da comunicare ex ante al Garante;

I diritti dell'interessato

Accesso e altri diritti (art. 7 e segg. del Codice)

Per l'esercizio di tali diritti

Non sono previste particolari modalità

Non è richiesta alcuna motivazione

- ✓ L'interessato e' tenuto unicamente a:
dimostrare la propria identità personale

- ✓ Il titolare non è tenuto a rilasciare copia degli atti ma a:
 - **estrarre dai propri archivi le informazioni analitiche che riguardano l'interessato.**
 - **renderle intellegibili.**
 - **dare tempestivo riscontro, anche negativo, all'interessato**

I diritti dell'interessato

Accesso e altri diritti (art. 7 e segg. del Codice)

(segue)

(Art.6 bis del d.lgs.322/89).

- “ L’aggiornamento, la rettificazione o l’integrazione dei dati sono annotati senza modificare questi ultimi qualora il risultato di tali operazioni non produca effetti significativi sull’analisi statistica o sui risultati statistici”
- In nessun caso si procede alla variazione dei dati se le modifiche richieste contrastano con le classificazioni e le metodologie statistiche adottate in base a norme internazionali, comunitarie e nazionali

Le misure di sicurezza

Art. 31 d.lgs. n. 196/2003

Obblighi di sicurezza

“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”

(segue) **Le misure di sicurezza**

Si tratta di un complesso di misure (tecniche, informatiche, organizzative, logistiche e procedurali) idonee a prevenire e ridurre al minimo il rischio di:

- distruzione o perdita dei dati
- accesso non autorizzato o trattamento non consentito

(segue) **Le misure di sicurezza**

Per sottrarsi alla responsabilità civile per danno il titolare deve dimostrare di aver adottato misure adeguate al livello di rischio rilevato

- **Art. 15 d.lgs. n. 196/2003**

“Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell’articolo 2050 del codice civile”*

- **Art. 2050 - Responsabilità per l'esercizio di attività pericolose**

Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.)

Le misure minime di sicurezza (artt.33-36 Codice)

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.

■ Gli standard per assicurare un livello minimo di protezione sono contenuti nel disciplinare tecnico allegato al Codice

■ La mancata adozione delle misure minime è punita con l'arresto fino a 2 anni o con l'ammenda da 10.000 a 50.000 euro. Ravvedimento operoso estingue reato (art. 169 del Codice).

(segue) **Le misure minime di sicurezza - Art. 34 del Codice**

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) 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.

Trattamenti senza l'ausilio di strumenti elettronici

- individuazione scritta degli incaricati e dell'ambito del trattamento consentito a ciascuno di essi, anche per classi omogenee di incarico (aggiornamento almeno annuale)
- istruzioni scritte agli incaricati per la custodia e la conservazione degli atti e documenti loro affidati in modo da evitare accessi non autorizzati
- conservazione dei documenti contenenti **dati sensibili e giudiziari** in archivi ad accesso controllato e disciplina delle modalità di accesso del personale autorizzato finalizzate alla identificazione degli incaricati

La «Politica di sicurezza» del Titolare

Scaturisce da un'attenta analisi volta a graduare la pericolosità del trattamento:

- il trattamento è automatizzato?;
- gli elaboratori sono accessibili in rete, le reti sono disponibili al pubblico?
- vengono trattati dati comuni o **dati sensibili e giudiziari?**
- il trattamento attiene a **dati idonei a rivelare lo stato di salute e la vita sessuale?**

(l'Istat adotta un «Documento annuale sulla sicurezza» anche in assenza di un espresso obbligo)

La protezione in alcune fasi del trattamento statistico:

- Raccolta
- Diffusione
- Comunicazione
- Conservazione

La protezione in alcune fasi del trattamento: la raccolta dei dati

(art. 10 del Codice di deontologia e di buona condotta)

Raccolta dei dati

1. *I soggetti di cui all'art. 1 pongono specifica attenzione nella selezione del personale incaricato della raccolta dei dati e nella definizione dell'organizzazione e delle modalità di rilevazione, in modo da garantire il rispetto del presente codice e la tutela dei diritti degli interessati, procedendo altresì alla designazione degli incaricati del trattamento, secondo le modalità di legge.*
2. *In ogni caso, il personale incaricato della raccolta si attiene alle disposizioni contenute nel presente codice e alle istruzioni ricevute. In particolare:*
 - a) *rende nota la propria identità, la propria funzione e le finalità della raccolta, anche attraverso adeguata documentazione;*
 - b) *fornisce le informazioni di cui all'art. 10 della legge e di cui all'art. 6 del presente codice, nonché ogni altro chiarimento che consenta all'interessato di rispondere in modo adeguato e consapevole, evitando comportamenti che possano configurarsi come artifici o indebite pressioni;*
 - c) *non svolge contestualmente presso gli stessi interessati attività di rilevazione di dati per conto di più titolari, salvo espressa autorizzazione;*
 - d) *provvede tempestivamente alla correzione degli errori e delle inesattezze delle informazioni acquisite nel corso della raccolta;*
 - e) *assicura una particolare diligenza nella raccolta di dati personali di cui agli articoli 22, 24 e 24-bis della legge.*

La protezione in alcune fasi del trattamento: la diffusione dei dati.

I dati personali possono essere **diffusi** solo in **forma aggregata** in modo che con l'impiego di mezzi ragionevoli non si possa risalire alla persona a cui i dati si riferiscono (**art. 9 d.lgs. n. 322/89- Segreto statistico**)

Il rischio di identificazione va valutato sulla base dei criteri indicati agli artt. 3 e 4 del Codice deontologico

Deroghe:

- Diffusione variabili pubbliche
- Diffusione variabili in forma disaggregata, espressamente indicate nel PSN

La protezione in alcune fasi del trattamento: la comunicazione dei dati

I soggetti SISTAN

possono **comunicare** i dati personali di cui siano venuti in possesso per scopi statistici:

- **ad altri enti e uffici di statistica del Sistan per fini statistici**
(v.slides 23-25);
- **a terzi estranei al Sistan per fini di ricerca scientifica**
(art. 7 del Codice deontologico*):
 - ✓ sotto forma di collezioni campionarie di dati individuali, che garantiscano comunque la non identificabilità dell'interessato;
 - ✓ in appositi laboratori di analisi di microdati (in Istat è attivo ADELE);
 - ✓ nell'ambito di progetti congiunti, previa stipula di protocolli di ricerca.

*L' «accesso per fini scientifici ai dati elementari raccolti per finalità statistiche» è ora disciplinato dall'art. 5-ter del d.lgs. n.33/2013. Il COMSTAT emana *Linee guida* per l'attuazione alla nuova disciplina

La protezione in alcune fasi del trattamento: la conservazione dei dati

In generale

I dati personali sono 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.

La protezione in alcune fasi del trattamento: la conservazione dei dati

In ambito Sistan

I dati personali sono di regola resi anonimi appena possibile e comunque al termine del trattamento

- Possono essere *conservati in forma personale* solo se idonei ad ulteriori trattamenti statistici
- In tale caso i *dati identificativi* devono essere conservati *separatamente* dalle altre informazioni
(a meno che ciò -in base ad atto motivato per iscritto- risulti impossibile per le particolari caratteristiche del trattamento o richieda l'impiego di mezzi sproporzionati)

Un problema connesso

La distruzione della modulistica utilizzata nel trattamento dei dati deve avvenire nel rispetto delle norme in materia di scarto dei documenti archivistici.