La *privacy* nella Pubblica Amministrazione e la sua tutela*

*di Giovanni Gioffré***

Premessa

Il codice per la protezione dei dati personali è stato approvato con decreto legislativo 30 giugno 2003, n. 196 ed è entrato in vigore il 1° gennaio del 2004. Successivamente è stato aggiornato dalla legge 18 marzo 2008, n. 48.

Il codice disciplina il trattamento dei dati personali, anche detenuti all'estero, effettuato a chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello "Stesso".

Il diritto alla protezione dei dati personali e il diritto alla riservatezza non coincidono; Il diritto alla riservatezza è il diritto di escludere altri dalla conoscenza di informazioni private, intime o familiari; è un diritto molto antico, e si fonda essenzialmente sul concetto de: "Il diritto di essere lasciato solo" o in maniera più drastica: "il diritto di essere lasciato in pace". Come dire: "In casa mia son re ed imperatore e ivi incontrastato ìmpero."

Questo diritto trova il suo fondamento storico e culturale nel diritto di proprietà; perciò stesso questo diritto tende ad escludere dal "godimento" che altri vengano a conoscenza di notizie o fatti ecc. Cioè quando il soggetto chiude "la porta di casa" metaforicamente parlando, nessuno ha più diritto di accesso.

Il diritto alla protezione dei dati personali è il diritto di esercitare un controllo sui dati e sulle informazioni che lo riguardano[1].

1. Diritto alla protezione dei dati personali

Il diritto alla riservatezza e il diritto alla protezione dei dati personali, dicevamo, sono diversi: entrambi diritti della personalità, entrambi assoluti, non cedibili, imprescrittibili ma a contenuto diverso.

Nel primo caso vi è il diritto alla riservatezza e le informazioni, appunto, riservate che si vogliono tenere escluse dalla conoscenza di altri; nel secondo si vogliono proteggere i dati e le informazioni. Il codice per la protezione dei dati personali non è necessariamente da considerarsi come una legge sulla *privacy*. Lo scopo, l'obiettivo invece è quello di regolamentare l'utilizzo delle informazioni: è una legge sull'utilizzo dell'informazione.

E' utile precisare che "le informazioni" non hanno un contenuto riservato, non c'è nessun riferimento ad un contenuto intimo, dato, familiare; queste informazioni possono essere anche informazioni pubbliche: per esempio il numero di telefono di un'utenza fissa,

1 Decreto legislativo 30 giugno 2003, n. 196, art. 1. *Diritto alla protezione dei dati personali.*
1. Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

pubblicato su un elenco telefonico, certamente non è un dato riservato però è un dato personale cioè una informazione soggetta al D.Lgs. n. 196/03.

I diritti che il soggetto può esercitare non sono soltanto a contenuto negativo, di escludere, ma anche di diritto positivo: di controllare, di accedere, di modificare, di integrare i propri dati.

L'art. 4 del decreto legislativo 30 giugno 2003, n 196 compendia tutte le definizioni di dati personali. Sinteticamente la definizione di dato personale è qualunque informazione riferibile direttamente o indirettamente a persona fisica, giuridica, ente, associazione.

Naturalmente ci possono essere dei dati personali che sono anche riservati, per esempio i dati sanitari contenuti nella cartella clinica: il dato personale è "l'informazione"[2].

Il legislatore italiano a differenza di quanto previsto dalla direttiva europea non ha limitato la definizione di dato personale alle persone fisiche ma l'ha estesa alle persone giuridiche, agli enti, alle associazioni; quindi nel nostro ordinamento giuridico il dato personale è l'informazione che si riferisce anche a enti, associazioni, pubblica amministrazione.

L'indirizzo del Ministero dell'Interno, poniamo, "piazzale del Viminale, n. 1 - 00184 Roma" è una dato personale e di riservato non c'è nulla, tutti lo sanno tutti lo possono sapere; ciò nondimeno è un dato personale.

L'Italia nel recepire la direttiva europea ha attuato una estensione del concetto di dato personale. La direttiva si riferiva a persone fisiche viventi.

Nel nostro ordinamento giuridico i dati personali sono tali anche se riferiti a persone decedute e questo è un problema molto più importante di quanto non si pensi a prima vista perché molti sono i casi di richiesta di informazione da parte degli eredi.

Per il codice non ha importanza il mezzo con cui si trattano i dati personali quindi se i dati vengono trattati con mezzi cartacei o informatici poco importa.

Dato personale non vuol dire "dato testuale"; dato personale non è necessariamente un dato scritto per cui la registrazione di immagini, il trattamento delle fotografie, le video riprese, la registrazione della voce sono tutte attività dove vengono trattati dati personali.

2. Il dato anonimo

L'art. 4 del decreto legislativo 30 giugno 2003, n 196 definisce il dato anonimo[3]. Al dato anonimo non si applicano gli istituti della norma di cui parliamo, quindi, niente informativa, niente indicazione dei responsabili, niente misure di sicurezza. Il dato

---

2 Decreto legislativo 30 giugno 2003, n. 196 art. 4, lett. b). Diritto *alla protezione dei dati personali*
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;

3 Decreto legislativo 30 giugno 2003, n. 196, art. 4, comma 1, lett. n):
n) «dato anonimo», il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

anonimo è in sintesi il dato che non può essere riferito ad un soggetto: persona fisica, persona giuridica, ente, associazione neanche indirettamente quindi un dato che non è riferibile ad un determinato soggetto. Il problema è stabilire quando il dato è anonimo.

Il dato anonimo o è stato raccolto sin dall'inizio in forma anonima oppure poi è stato elaborato per trasformarlo in dato anonimo. Quindi il dato non è anonimo nel senso di essere etimologicamente privo del nome, non basta che sia privo del nome perché si possa considerare anonimo nel senso del codice per l'applicazione dei dati personali; deve essere "non collegabile" ad un soggetto.

Nella vita di ogni giorno può capitare di imbattersi in questionari. Nella maggior parte dei casi non si è certi che si tratti di questionari effettivamente anonimi se si inseriscono delle informazioni che sono collegabili al soggetto che risponde. Quando si può affermare che il dato è anonimo?

A tale proposito si tende a dare la seguente risposta: se il dato sia anonimo o no è cosa che va misurata con riferimento al tempo, alle risorse, alle misure tecnologiche necessarie per "ritrasformare" il dato anonimo in dato identificativo. Se la "ritrasformazione" del dato è questione abbastanza semplice da risolvere il dato non è anonimo se invece trasformare il dato anonimo in dato identificativo richiede tempo, risorse economiche e mezzi tecnologici elevati allora il dato si può considerare anonimo. Il concetto di "anonimo" non è una concetto definibile drasticamente: bianco-nero; è un concetto graduabile, che cambia e si misura a seconda delle circostanze.

3. Dati sensibili

La lettera d) dell'art. 4 del decreto legislativo 30 giugno 2003, n 196 individua il dato sensibile[4]. In sintesi si può dire che i dati sensibili sono quelli donde rilevare l'origine etnica, le opinioni politiche, sindacali, la fede religiosa, lo stato di salute, la vita sessuale.

I dati sensibili non sono dati che "rivelano" ma sono dati "idonei a rivelare", secondo la definizione del codice. Per esempio un alunno che a mensa abbia rivelato come preferenza alimentare di non mangiare certi cibi può essere un bambino che ha certe allergie quindi è un dato sensibile perché ricade nello stato di salute. Oppure un bambino la cui famiglia aderisce ad una determinata fede religiosa e quindi comunque un dato sensibile.

Un dato quindi che di per sé non rivela la salute né la fede religiosa ma diventa sensibile perché, all'analisi, è idoneo a "rivelare".

Non sono sensibili, nell'ordinamento giuridico italiano, i dati economici e finanziari, i dati riferiti al reddito, i redditi di una persona, i compensi che questa percepisce, l'ammontare del suo conto corrente, il suo patrimonio azionario o che dir si voglia. Sotto il

4 Decreto legislativo 30 giugno 2003, n. 196, art. 4, comma 1, lett. d):
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;

profilo strettamente giuridico questi non sono dati sensibili. Questi dati saranno quindi trattati come dati personali. Naturalmente la nostra dichiarazione dei redditi può contenere dei dati sensibili: La scelta del cinque per mille è un dato sensibile, se inseriamo dei dati sanitari quelli possono essere un dato sensibile.

4. Trattamento dei dati personali.

La lettera a) del solito art. 4 del decreto legislativo 30 giugno 2003, n 196 definisce cosa si intende per trattamento dei dati personali.

In breve il trattamento sostanzialmente è ogni operazione effettuata sui dati. Il trattamento dei dati deve avvenire secondo il dettato dell'art. 11 del codice cioè devono essere trattati in modo lecito, secondo correttezza, per scopi determinati, esatti e se necessario essere aggiornati, pertinenti rispetto alle finalità per le quali vengono raccolti e trattati, conservati in una forma che consenta l'identificazione dell'interessato e per un tempo determinato.

Trattamento non necessariamente è sinonimo di elaborazione. Infatti, anche la sola conservazione in modo assolutamente passivo dei dati costituisce comunque trattamento. Supponiamo che un Comune abbia un archivio cartaceo che è depositato in una luogo addirittura diverso dal punto di vista fisico rispetto a quello in cui c'è la sede operativa, supponiamo anche che questo archivio cartaceo non sia mai praticamente consultato, comunque conservare quei dati nell'archivio è "trattamento". Quindi trattamento non significa elaborare, lavorare il dato, associare delle informazioni, modificarlo. Trattamento e anche la mera lettura e la mera visualizzazione dei dati anche se temporanea.

Particolare rilievo oggi assume la video sorveglianza. Come lo stesso Garante ha evidenziato sono stati sottoposti all'esame dell'Autorità numerosi casi, attraverso reclami, segnalazioni e richieste di parere, i quali evidenziano un utilizzo crescente, spesso non conforme alla legge, di apparecchiature audiovisive che rilevano in modo continuativo immagini, eventualmente associate a suoni, relative a persone identificabili, spesso anche con registrazione e conservazione dei dati. Il Garante ponendo doverosa attenzione al nuovo diritto alla protezione dei dati personali, consacrato all'art. 1 del codice, ha ritenuto di intervenire emanando il provvedimento a carattere generale del 29 aprile 2004 sulla materia inerente la videosorveglianza.

Tra i principi generali il Garante ha inserito il principio di liceità secondo il quale il trattamento dei dati attraverso sistemi di videosorveglianza è possibile solo se è fondato su uno dei presupposti di liceità che il Codice prevede espressamente.

Il principio della necessità secondo il quale, poiché l'installazione di un sistema di videosorveglianza comporta in sostanza una limitazione e comunque un condizionamento per il cittadino va escluso ogni uso superfluo ed evitati eccessi e ridondanze.

Il principio di proporzionalità, cioè va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorre un'effettiva esigenza di deterrenza, come quando, ad esempio, le telecamere vengono installate solo per meri fini di apparenza o di "prestigio".

Il principio di finalità secondo il quale gli scopi perseguiti devono essere determinati, espliciti e legittimi (art. 11, comma 1, lett. b), del Codice). Ciò comporta che il titolare possa perseguire solo finalità di sua pertinenza.

Quando per un qualsiasi motivo il trattamento cessa i dati devono essere distrutti.

5. Comunicazione e diffusione

La comunicazione e la diffusione sono due termini importanti per la pubblica amministrazione e significano rispettivamente dare conoscenza al soggetto determinato quindi dare conoscenza ad una persona fisica o giuridica indifferente determinata, per esempio al soggetto che richiede l'accesso *ex* legge n. 241/90 che accede ad una comunicazione ai sensi del decreto legislativo 30 giugno 2003, n 196.

Mentre invece la diffusione è dare conoscenza a soggetti indeterminati per esempio pubblicandoli. La pubblicazione della dichiarazione dei redditi da parte dell'agenzia delle entrate su Internet è sicuramente un caso di diffusione. E a tale proposito il garante ha ritenuto illegittima la diffusione dei dati sul sito Internet dell'agenzia delle entrate[5].

Pubblicare all'albo pretorio, pubblicare su Internet, pubblicare su un bollettino, sono tutte forme di diffusione senza però conoscere il destinatario: il destinatario è indeterminato.

---

5 A tale proposito il Garante nel provvedimento del 6 maggio 2008, tra l'altro, ha sostenuto che il provvedimento del Direttore dell'Agenzia poteva stabilire solo *"i termini e le modalità"* per la formazione degli elenchi. La conoscibilità di questi ultimi è infatti regolata direttamente da disposizione di legge che prevede, quale unica modalità, la distribuzione di tali elenchi ai soli uffici territorialmente competenti dell'Agenzia e la loro trasmissione, anche mediante supporti magnetici ovvero sistemi telematici, ai soli comuni interessati, in entrambi i casi in relazione ai soli contribuenti dell'ambito territoriale interessato. Ciò, come sopra osservato, ai fini del loro deposito per la durata di un anno e della loro consultazione –senza che sia prevista la facoltà di estrarne copia da parte di chiunque *(art. 69, commi 4 ss., D.P.R. n. 600/1973 cit.; v. anche art. 66 bis D.P.R. 26 ottobre 1972, n. 633)*; la predetta messa in circolazione in Internet dei dati, oltre a essere di per sé illegittima perché carente di una base giuridica e disposta senza metterne a conoscenza il Garante, ha comportato anche una modalità di diffusione sproporzionata in rapporto alle finalità per le quali l'attuale disciplina prevede una relativa trasparenza. I dati sono stati resi consultabili non presso ciascun ambito territoriale interessato, ma liberamente su tutto il territorio nazionale e all'estero. L'innovatività di tale modalità, emergente dalle stesse deduzioni dell'Agenzia, non traspariva dalla generica informativa resa ai contribuenti nei modelli di dichiarazione per l'anno 2005. L'Agenzia non ha previsto "filtri" nella consultazione *on-line* e ha reso possibile ai numerosissimi utenti del sito salvare una copia degli elenchi con funzioni di trasferimento *file*. La centralizzazione della consultazione a livello nazionale ha consentito ai medesimi utenti, già nel ristretto numero di ore in cui la predetta sezione del sito *web* è risultata consultabile, di accedere a innumerevoli dati di tutti i contribuenti, di estrarne copia, di formare archivi, modificare ed elaborare i dati stessi, di creare liste di profilazione e immettere tali informazioni in ulteriore circolazione in rete, nonché, in alcuni casi, in vendita. Con ciò ponendo anche a rischio l'esattezza dei dati e precludendo ogni possibilità di garantire che essi non siano consultabili trascorso l'anno previsto dalla menzionata norma;

6. Titolari e responsabili incaricati

Si intende per «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[6].

Nel caso specifico è la pubblica amministrazione è il Comune, è l'ente, è il soggetto che assume decisioni con riferimento a finalità, modalità di trattamento e sicurezza.

Qualora più enti partecipano a un determinato progetto di trattamento dei dati il criterio per determinare il titolare può essere riferibile al soggetto che adotta le decisioni in materia di sicurezza dei dati personali.

Ci sono molte varianti ad un titolare unico che decide e le varianti sono: la contitolarità; cioè ci possono essere dei casi in cui più soggetti, unitamente, trattano i dati personali. Più comuni insieme decidono di costituire una nuova banca dati nella quale confluiscono dati di determinate categorie di cittadini, nel creare questa nuova banca dati i comuni suddetti co-gestiscono tutte le decisioni. Siamo nel caso di contitolarità cioè più titolari associati.

E' chiaro che nel caso di contitolarità è necessaria la predisposizione di un'informativa congiunta nei confronti del cittadino, designazione congiunta di incaricati e responsabili, documento programmatico per la sicurezza congiunto. Cogestione significa anche osservanza di tutti gli adempimenti della legge per la protezione dei dati personali. E' appena il caso di evidenziare che quanto sopra è molto oneroso da gestire, sotto il profilo operativo, tuttavia è una ipotesi possibile. Un'altra ipotesi possibile è la comunicazione tra due soggetti che siano entrambi titolari, in questo caso ciascuno rimane titolare dei suoi dati e se li comunicano. Questo è il caso di titolarità autonoma.

In questo caso chi si occupa dei dati che lo riguardano, sono tutti e due i soggetti autonomi, nessuno risponde di ciò che fa l'altro. Quindi nessuno dei due si deve occupare di dare l'informativa agli interessati per quello che fa l'altro, di nominare incaricati, di nominare responsabili di redigere il documento programmatico per la sicurezza è in definitiva una situazione completamente diversa rispetto a quella della "contitolarità."

Chi è titolare è anche responsabile. Nel caso specifico il titolare è il responsabile di tutti gli adempimenti previsti dal D.Lgs. n. 196/03, può, non deve, può designare incaricati, fornire ad essi istruzioni, direttive. risponde comunque per la scelta, la vigilanza e controllo e per ciò stesso non si libera mai completamente della responsabilità. Ci sono una serie di obblighi del titolare previsti dalla legge.

La lett. g), dell'art. 4 del codice stabilisce che il "responsabile", può essere una persona fisica una persona o giuridica, può essere uno soggetto privato o soggetto pubblico, ed è il soggetto che è designato, preposto, da titolare, specificamente a uno o più trattamenti di dati personali.

Ai sensi dell'art. 29, comma 1, del D.Lgs n. 196/03[7], questo soggetto è figura facoltativa e

---

6 Decreto legislativo 30 giugno 2003, n 196, ar. 4, comma 1, lett.f).

7 Decreto legislativo 30 giugno 2003, n 196, art 29. *Responsabile del trattamento.*

non necessariamente unica perché non è detto che ci sia uno solo responsabile, anzi, possono esserci molti più responsabili per un medesimo trattamento. Per esempio ci può essere un responsabile dal punto di vista informatico, un responsabile dello stesso trattamento sotto il profilo strettamente giuridico. Il medesimo articolo al comma 4 prescrive che il responsabile sia designato per iscritto e che i compiti del responsabile siano specificamente individuati. A nulla vale la declinazione del tipo "il signor Rossi è designato responsabile per la sicurezza dell'ente" oppure "responsabile per la sicurezza dei dati personali nell'ente." Occorre che le istruzioni siano specifiche. Il responsabile può essere anche una pubblica amministrazione, può essere una persona fisica come una persona giuridica. Il responsabile non necessariamente deve essere designato con atto individuale; il nominativo può essere designato anche con atto di natura generale: un regolamento può designare il responsabile con riferimento ai ruoli ricoperti dai vari soggetti all'interno dell'ente.

I responsabili possono essere individuati anche all'esterno all'amministrazione. Oggi sempre più spesso sono, soggetti esterni alla pubblica amministrazione; cioè soggetti che per conto della stessa o comunque svolgendo delle operazioni che rientrano negli interessi della pubblica amministrazione rispetto ai quali sono stati incaricati o rispetto alle quali sono contraenti trattano dati personali della pubblica amministrazione di cui è titolare la pubblica amministrazione.

Può essere il caso di una impresa che svolge presso un nostro Comune la manutenzione dei sistemi informativi. In questa eventualità, questa impresa tratterà i dati informatici di cui il comune è il titolare; oppure può essere l'esempio del tesoriere che eroga gli stipendi. In questi casi si può configurare questo soggetto come un responsabile del trattamento.

Si faceva l'esempio del tesoriere che eroga gli stipendi. Orbene poniamo che il tesoriere sia una banca. Se la banca si occupa di erogare i compensi, in questo caso, esercita una attività che è propria dell'ente. In questa veste di responsabile è ovvio che non debba fornire una informativa all'interessato né tanto meno chiedere il consenso. Essa svolge la sua attività quale braccio operativo con le finalità del Comune.

Supponiamo però che la banca ad un certo punto invii a soggetti con cui comunica, in quanto contraente del comune, proposte di investimenti finanziari. Questo non rientra più tra le finalità proprie del Comune. A questo punto la banca sta operando autonomamente scegliendo nuove finalità di trattamento. Non agisce più quale responsabile del trattamento per conto del Comune. In questo momento agisce quale novo titolare di trattamento e in quanto tale, conformemente alle disposizioni della legge sul 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

dei dati personali, dovrà inviare una informativa all'interessato, chiedere il consenso al trattamento dal momento che è un soggetto privato.

Dal punto di vista normativo, l'articolo 29, che fa riferimento ai responsabili nulla ci dice sui compiti dei responsabili. Quindi, compiti e responsabilità dei responsabili vanno misurate solo ed esclusivamente sull'atto di designazione degli stessi. Gli incaricati, ai sensi dell'art. dell'art. 4 lett. h) del D.Lgs. n. 196/03, sono necessariamente persone fisiche non possono essere persone giuridiche.

La designazione di "incaricato" deve essere effettuata per iscritto e deve essere analitica. Gli incaricati non sono necessariamente dipendenti ma possono essere dei collaboratori temporanei, corsisti, volontari. Qualora il responsabile per i dati e non è stato designato come responsabile comunque ne risponde il titolare.

7. Misure di sicurezza

I dati devono essere coperti da misure di sicurezza posti in essere per evitare alcuni rischi che possono essere rischi di danneggiamento, di distruzione, di accesso non autorizzato. Rischi precisati dal legislatore nell'articolo 31. Questi rischi riguardano tutti i dati personali sensibili e non sensibili, tutti i dati trattati con mezzi informatici e non; sia il rischio di allagamento, di un incendio sia il rischio da pirati informatici.

Le misure di sicurezza si dividono sostanzialmente i due tipologie misure di sicurezza da adottare per evitare la responsabilità civile e misure di sicurezza da adottare per evitare la responsabilità penale.

Responsabilità civile. Il nostro legislatore ha fatto riferimento alla disposizione più rigorosa del nostro codice civile cioè responsabilità per l'esercizio di attività pericolosa, avuto riguardo alla natura dei mezzi adoperati, inversione dell'onere della prova, responsabilità oggettiva. Quindi il danneggiato dovrà provare solo il fatto e il danno e il nesso di causalità mentre il danneggiante, per liberarsi da responsabilità e contestazioni, dovrà dare la difficilissima prova di aver adottato tutte le misure idonee ad evitare il danno.

8. Misure minime di sicurezza

Le misure minime di sicurezza sono espressamente elencate nell'allegato B. del codice della protezione dei dati personali intitolato "disciplinare tecnico in materia di sicurezza."

L'allegato B del codice prevede, tra le misure minime di sicurezza che l'aggiornamento delle liste degli incaricati sia almeno annuale. Le misure minime riguardano le modalità di trattamento; cioè sia i trattamenti effettuati con mezzi informatici e non, che da tempo ormai dovevano essere adottati.

L'aggiornamento può consistere in una conferma delle liste degli incaricati e con ciò si adempie a quanto prescritto.

Gli incaricati sono coloro che accedono ai dati anche con mezzi informatici, anche

attraverso una password e quindi il presupposto del controllo e il monitoraggio delle password inevitabilmente passa attraverso la individuazione di incaricati. Le password devono essere aggiornate ogni tre o sei mesi.

La mancata adozione delle misure minime di sicurezza ha conseguenze di natura penale ai sensi dell'articolo 169: «reato di omissione di adozione di misure di sicurezza e pertanto si configura per la semplice mancata adozione delle misure di sicurezza e non occorre anche il danneggiamento di un determinato soggetto». L'Articolo citato prevede una forma di ravvedimento operoso cioè se si verifica che un determinato titolare non ha adottato le misure minime di sicurezza, allo stesso può essere assegnato un termine, massimo sei mesi, entro cui il soggetto deve provvedere. Se questi nei sessanta giorni successivi, allo scadere del termine, provvede a quanto prescritto è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione[8]. L'adempimento e il pagamento estinguono il reato.

9. Diritti dell'interessato

Il soggetto interessato, i cui dati sono trattati, ai sensi dell'art. 13 del codice, ha diritto di ricevere un'informativa, la quale può essere scritta o orale, può essere anche generale, cioè può essere resa attraverso un cartello, non ci sono particolari formalità. L'informativa deve contenere il contenuto minimo, finalità e modalità di trattamento.

Al soggetto interessato deve essere comunicato chi è "il responsabile per il riscontro delle notizie all'interessato"; cioè il soggetto a cui rivolgersi per far valere i propri diritti.

La omessa o inidonea informativa all'interessato, ai sensi dell'art. 161 del codice, comporta una sanzione amministrativa che può arrivare a 90.000 euro. Quindi la omessa completa informativa è sanzionata. È un obbligo la cui inosservanza, a differenza della legge precedente dove questa sanzione non era prevista, con il D.Lgs. n. 196/03, è particolarmente e severamente sanzionato.

L'interessato ha diritto di ottenere la conferma della comunicazione dei dati che lo riguardano: può chiedere alla P.A. e nel caso specifico al comune, di sapere quali dei suoi dati sono trattati e può chiedere di avere copia di questi dati.

La richiesta può essere anche esercitata nei confronti dell'ASL e consistere nella domanda di rilascio di copia della eventuale registrazione dell'intervento chirurgico subito

---

8 Decreto legislativo 30 giugno 2003, n. 196. Art. 169. *Misure di sicurezza.*
1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.
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 dell'ammenda stabilita per la contravvenzione. 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.

dall'interessato.

Supponiamo che ci sia una forma di video sorveglianza: può chiedere, poniamo al comune che le detiene, di avere, appunto, accesso a quelle immagini.

L'interessato può chiedere anche che gli sia resa nota la fonte da dove provengono questi dati, presso chi sono stati raccolti e può chiedere che siano rese note finalità, molti dei dati di trattamento, logica del trattamento.

L'interessato può chiedere l'aggiornamento, la rettifica, l'integrazione dei dati e se i dati erronei sono stati portati a conoscenza di terzi può chiedere che ai terzi siano comunicati i dati corretti e può anche chiedere l'attestazione che le correzioni siano state effettivamente comunicate ai terzi. L'interessato ha diritto in questo caso motivando di opporsi al trattamento dei dati cioè ove ricorrano particolari ragioni può richiedere che il suo trattamento dei suoi dati sia sospeso. Qualora i dati siano trattati per finalità di marketing, per pubblicità, per esigenze commerciali può sempre opporsi al trattamento.

10. Modalità di esercizio dei diritti

L'interessato può rivolgersi al titolare e in particolare al responsabile del riscontro degli interessati se è stato indicato nell' informativa, direttamente, recandosi di persona presso l'ufficio, deve essere adeguatamente identificato dal titolare.

Se la richiesta è una richiesta che viene effettuata attraverso qualche altro mezzo per esempio un mezzo postale per raccomandata, ovviamente sarà allegato uno al documento di riconoscimento; nell'e-mail con firma digitale sarà sufficiente la firma digitale.

Dubbi sussistono con riferimento soltanto alla comunicazione telefonica. Cioè se la richiesta viene effettuata in maniera telefonica, con i mezzi telefonici c'è il problema della identificazione.

La richiesta può essere esercitata anche da altri per l'interessato e quindi l'interessato può rilasciare procura, delega ad altri che provvederanno il suo nome.

La persona che agisce per conto dell'interessato esibisce o allega copia della procura, della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata del documento di identità.

Naturalmente come detto prima l'interessato, per la legge italiana, può esercitare questo diritto di accesso ai dati anche per le persone decedute.

In questo caso, nella pratica, riguarda di solito problemi di eredità. Quindi le informazioni relative alle persone decedute possono essere comunicate anche ai familiari nei casi previsti dall'articolo nove.

La richiesta dell'interessato deve essere evasa entro quindici giorni prorogabili a trenta giorni in casi di particolare complessità previa comunicazione all'interessato. Se la richiesta è presentata oralmente deve essere verbalizzata.

Se l'ente non adempie l'interessato può fare ricorso al garante il quale in tempi abbastanza rapidi decide.

Il garante non indica il risarcimento del danno; questo è di competenza del tribunale presso cui ha sede il titolare ma liquida invece le spese amministrative e contabili e questo

può comportare una responsabilità contabile qualora non si sia, nei tempi previsti dalla legge, risposto alla richiesta.

11. L'aspetto penale.

L'art. 167 prevede la reclusione da sei a diciotto mesi per chiunque procede al trattamento dei dati personali, al fine di trarne profitto per se o per altri, o arrecare ad altri un danno, in violazione degli art. 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'art. 129. Se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi. Il trattamento illecito dei dati personali. Perché si verifichi questo reato occorre il concorso di tre elementi essenziali che si devono verificare contestualmente. Primo: il trattamento deve essere illecito cioè per esempio effettuato non conformemente ai fini istituzionali della P.A., nel caso specifico, del Comune. Secondo elemento: dolo specifico. Cioè volontà di procurare ad altri un danno o trarne profitto; terzo elemento: effettivo nocumento all'interessato. Solo se contestualmente questi tre requisiti si realizzano si prospetta l'ipotesi del reato di trattamento illecito dei dati personali.

In generale, si può dire che si concretizza un reato quando ci si trova di fronte a comunicazione indesiderata di dati. Spessissimo, da parte di tantissime ditte commerciali, vengono spedite via e-mail o via fax, messaggi che pubblicizzano un determinato prodotto senza che i destinatari abbiano prestato il consenso. Si realizza innanzitutto una trattamento illecito dei dati personali perché si trattano i dati senza consenso ed ecco il verificarsi del primo presupposto; Con l'invio di questi messaggi pubblicitari viene ampliato il mercato delle suddette imprese commerciali quindi il fine di lucro implicito; ecco che si verifica il secondo presupposto (..Al fine di trarne profitto per se… si diceva prima). Infine si arreca un nocumento perché come la nostra giurisprudenza ha affermato si viola il diritto di un soggetto ad essere lasciato in pace, il diritto alla riservatezza.

12. Omessa osservanza dei provvedimenti del garante

Infine, l'art. 170 del codice commina anche una sanzione penale, prevedendo la punizione della reclusione da tre mesi a due anni per la mancata osservanza del provvedimento del Garante adottato ai sensi dell'art. 26 comma 2, 90, 150, commi 1 e 2, 1 43, comma 1 lett. c), del medesimo codice.

<<<<<<<<<<§>>>>>>>>>>

** In "Diritto & Diritti" – Rivista giuridica elettronica, pubblicata su Internet all'indirizzo http://www.diritto.it, ISSN 1127-8579, Settembre 2008, pag. http:// www.diritto.it/art.php?file=/archivio/26450.html e segg.;*

*** Segretario Generale della Città di Norcia (PG)*