IL CODICE PER LA PROTEZIONE DEI DATI PERSONALI

D. LGS 196/03
Art. 1, 3, 4, 5, 7, 8, 11, 13, 15, 16, 18, 19, 20, 23, 24, 26, 29, 30, 33, 34, 37, 42, 43, 44, 161, 163, 167, 168, 169

Codice Civile (CC): 2043, 2050, 1226
Codice Procedura Civile (CPC): 700

Riferimenti ulteriori:
Diritto di Internet, G. Finocchiaro: capitolo IV.

1. IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

D. LGS 2003 nro 196

La prima legge in materia di protezione dei personali in Italia è stata emanata alla fine del 1996: possedere una legge in merito era necessario come condizione per aderire all'accordo di Schengen sulla libera circolazione delle persone aveva già firmato nel 1990 e che era entrato in vigore dal 1995.

Le norme sulla privacy e la tutela dei dati personali sono state raccolte nel Codice attuale nel 2003.

Art. 1. Diritto alla protezione dei dati personali

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

Le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto ad una funzione pubblica e la relativa valutazione non sono oggetto di protezione della riservatezza personale.

Art. 4 comma 1 Definizioni

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;

Il diritto alla protezione dei dati personali è il diritto a vedere protetta qualunque informazione su un soggetto, riferibile a un soggetto. Un dato personale è qualunque dato che identifica un soggetto, non necessariamente riservato o privato, come ad esempio nome o numero di matricola, ma anche peso, altezza, voce, partita IVA. Anche la musica che una persona ascolta è un dato personale, così come un colloquio, una dichiarazione, un'opinione o manifestazione del pensiero, in qualunque forma o supporto.

Il dato personale è quindi caratterizzato dalla massima generalità, ed è tale indipendentemente dalla volontà del soggetto a cui è riferito di renderlo pubblico o meno. I dati personali sono dati che permettono un'identificazione sia immediata (come ad esempio i dati anagrafici), sia mediante collegamento con altre informazioni.

Mentre dal punto di vista informatico un dato personale è un'informazione, dal punto di vista giuridico il dato personale può anche non veicolare informazione di per se stesso.

Nella legislazione italiana anche enti e associazioni (persone giuridiche) hanno diritto alla protezione dei loro dati personali, ad esempio numero di iscrizione alla camera di commercio, numero di partita IVA, bilancio, nomi dei componenti del consiglio di amministrazione..

Diritto alla protezione dei dati personali e diritto alla riservatezza

La legge sulla protezione dei dati personali non è una legge sulla protezione della riservatezza, quella che nel linguaggio comune chiamiamo privacy, bensì sull'uso dell'informazione, sulla circolazione dell'informazione.

Il dato personale non comprende il concetto di riservatezza.

Il diritto alla riservatezza è il diritto di una persona di vedere riservate, non pubbliche, non utilizzate e non conosciute, informazioni intime, private o familiari (una sfera più ristretta rispetto ai dati personali), ed è un diritto distinto da quello della protezione dei dati personali. La riservatezza è protetta dalla giurisprudenza (es. sentenze Cassazione).

Alcuni dati personali sono anche soggetti al diritto alla riservatezza, come ad esempio il contenuto di una cartella clinica o le operazioni del proprio conto corrente, ma non tutti.

Il diritto alla riservatezza nasce nell'800 negli USA (e nello stesso periodo in Germania), con la richiesta di un senatore di Boston di non veder continuamente pubblicate notizie sulla vita mondana della moglie. Il diritto alla riservatezza è una specie di diritto di proprietà: si considera

che la propria vita privata sia una proprietà, e come tale sia possibile escluderne gli altri (“the right to be let alone”). Questo diritto dà luogo a una libertà negativa, ha contenuto negativo: si escludono gli altri dalla conoscenza.

Il diritto alla protezione dei dati personali è invece un diritto positivo, di agire: è il diritto della persona di esercitare un controllo sulle informazioni che la riguardano (conoscerle, correggerle, consentirne o meno l'uso, averne copia..).

Entrambi i diritti sono diritti della personalità e come tali assoluti (possono essere fatti valere su ogni soggetto), imprescrittibili (non soggetto a prescrizione se non fatti valere) e indisponibili (non possono essere oggetto di contratto, non possono essere ceduti o alienati). I diritti della personalità si considerano riconosciuti, *trovati*, dal diritto, e non creati da esso.

Esiste un terzo diritto della personalità che ha margini di sovrapposizione col diritto alla protezione dei dati personali e diritto alla riservatezza, e si deve quindi citare: il diritto all'identità personale. Il diritto all'identità personale è il diritto a non veder travisata la propria immagine sociale, politica, in generale ideologica. Questo diritto protegge in un certo senso il concetto di personalità dell'individuo (là dove il diritto al nome protegge il suo nome e il diritto all'immagine la sua immagine fisica, concetti più “concreti”), e viene violato non solo con l'attribuzione di notizie false su una persona ma anche di notizie vere ma riportate in un modo tale che il loro significato ne risulti travisato.

Il diritto alla protezione dei dati personali è sancito dall'Art. 1 del d. lgs. 196/03.

Il lavoro dei pubblici funzionari non è oggetto di protezione dei dati personali. Questa frase, aggiunta nel marzo 2009, è scritta molto male dal punto di vista giuridico, e per questa ragione pone molti problemi applicativi: la riservatezza non non c'entra con la protezione dei dati personali di cui parla il d. lgs. 196/03, e inoltre la riservatezza non è personale.

1.2 DATI ANONIMI

Art 4 comma 1

n) "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile

Che cosa non è dato personale? Non è dato personale un'informazione non collegabile a un soggetto, ad esempio dati aggregati, informazioni depurate di nomi.. Quel che non è dato personale è detto **dato anonimo**.

Solo i dati anonimi non rientrano nell'ambito applicativo del d. lgs. 196/03.

La criterio secondo il quale un dato è personale o anonimo è la collegabilità ad un soggetto, e questa associazione potenziale varia a seconda delle circostanze. Si pensi ad esempio a dati raccolti in forma anonima in una classe, che chiedano opinioni sulla qualità della didattica. Una domanda sul sesso del soggetto che compila il questionario può non permettere alcuna collegabilità dei dati a un soggetto specifico, ma non se nella classe vi fosse un solo studente di sesso femminile. In questa eventualità, i dati non sarebbero dati anonimi per quello studente.

La collegabilità è un criterio elastico che si articola diversamente a seconda dei casi o dei costi, in altre parole l'anonimia del dato va valutata caso per caso a seconda dei mezzi e delle situazioni reali. Potenzialmente moltissime informazioni possono essere dati personali.

Un dato anonimo può essere raccolto così, privo di riferimenti, o reso anonimo successivamente, privandolo dei riferimenti.

1.3 DATI SENSIBILI E GIUDIZIARI

Art. 4 comma 1

d) "**dati sensibili**", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e) "**dati giudiziari**", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

I dati sensibili sono quelli che riguardano la personalità etico-sociale dell'individuo e le sue caratteristiche psico-sanitarie.

I dati sensibili sono definiti sulla base di un elenco tassativo, chiuso, e non esemplificativo, ma suscettibile di interpretazione elastica, per via del “idoneo a rivelare”. Ad esempio il fatto che qualcuno non mangi certi alimenti può rivelare la fede religiosa o lo stato di salute, ma può anche essere solo rivelatorio di gusti in fatto di cibo. La playlist delle canzoni su un iPod può potenzialmente essere anch'essa dato sensibile: può esprimere convinzioni politiche e religiose, se contiene canzoni con forti connotazioni in tali sensi.

Esempi classici di dati sensibili possono essere quelli contenuti in una cartella clinica, o l'adesione a un club politico, o il velo portato da una donna. Il reddito e i vari dati di tipo economico/patrimoniale sono dati personali ma non sono dati sensibili.

Nella definizione di dato sensibile appare anche il concetto generale di “convinzione filosofica”, che non ha una sua precisa definizione: in questa categoria si possono far rientrare ad esempio convinzioni di tipo ambientalista, che possono in qualche modo essere considerate “idee filosofiche”.

I soggetti pubblici possono trattare dati personali solo nei casi in cui strettamente necessario per i singoli scopi, controllando periodicamente la pertinenza, non eccedenza, e necessità del trattamento di tali dati rispetto alle finalità.

Il trattamento illecito di dati sensibili è considerato più grave rispetto a quello di dati personali non sensibili, e devono essere trattati con tecniche di cifratura o con l'utilizzazione di codici identificativi, in modo da poter identificare gli interessati solo in caso di necessità.

I dati sensibili atti a rivelare lo stato di salute o la vita sessuale di una persona devono essere conservati separatamente da ogni altro dato personale trattato (Art. 22 comma 7), e i primi non possono in nessuna circostanza essere diffusi (Art. 22 comma 8, Art. 26 comma 5).

I dati giudiziari sono ad esempio i provvedimenti giudiziari definitivi di condanna o concernenti le pene o la riabilitazione, i provvedimenti di interdizione e inabilitazione, e anche la qualità di imputato o indagato. I dati giudiziari sono disciplinati come i dati sensibili.

A volte si indicano i dati personali non sensibili e non giudiziari come dati comuni, termine che però non appare mai nel Codice.

1.4 TRATTAMENTO

Art 4 comma 1

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

l) "**comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

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

Cos'è un trattamento di dati personali? Tutte le operazioni sui dati personali, sia informatizzati che cartacei, costituiscono trattamento, non vi sono operazioni escluse. Il trattamento non dipende da una qualche elaborazione che si fa sui dati, sono trattamento anche la lettura o la mera conservazione. Il Codice in materia di protezione dei dati personali ha quindi un campo di applicazione estremamente vasto.

Il collegamento di un'informazione al soggetto a cui si riferisce, senza avere il diritto di farlo, costituisce trattamento illecito. Il solo dato non è mai illecito in sé, ma può esserlo il relazione ai trattamenti e ai soggetti coinvolti nel trattamento.

Due operazioni sui dati personali hanno ricevuto particolare specifica definizione legislativa: la comunicazione e la diffusione.

La comunicazione è il trattamento che si ha quando i dati sono comunicati a uno o più soggetti determinati o determinabili (es. dati comunicati a una o più persone specifiche via email, dati resi noti a tutti i dipendenti, dati esposti in un area accessibile solo da soggetti noti e autorizzati).

La comunicazione avviene solo quando i dati sono trasmessi tra titolari di trattamento autonomi. Non si ha comunicazione quando i dati vengono trasmessi tra responsabili e incaricati, ad esempio.

La diffusione si ha quando i dati sono comunicati a soggetti indeterminati o potenzialmente infiniti (es. un foglio esposto, o la pubblicazione su internet). Il criterio secondo cui si distingue tra comunicazione e diffusione è la possibile identificazione del destinatario.

Art. 16. Cessazione del trattamento

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:
   a) distrutti;
   b) ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
   c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
   d) conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi de all'articolo 12.
2. La cessione dei dati in violazione di quanto previsto dal comma 1, lettera b), o di altre disposizioni rilevanti in materia di trattamento dei dati personali è priva di effetti.

È necessario notificare all'autorità Garante la cessazione del trattamento, attraverso l'apposito modulo predisposto su supporto informatico.

La cessazione del trattamento si ha quando il titolare intende interrompere definitivamente tutte le operazioni relative a un determinato trattamento di dati. Ad esempio, non si ha cessazione quando una pubblica amministrazione sopprime un singolo archivio ritenuto inutile, pur continuando il trattamento di dati nel complesso.

1.5 L'AUTORITA GARANTE PER LA PRIVACY

Art 4 comma 1

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

Organo collegiale di nomina parlamentare con sede a Roma, composto di quattro membri i quali eleggono tra loro un presidente. Il presidente attuale è Pizzetti, il precedente è stato Rodotà. Attualmente ha 125 funzionari.

Effettua ispezioni direttamente o avvalendosi della guardia di finanza, e ha la facoltà di erogare sanzioni ai sensi dell'Art. 154. Il Garante non può liquidare i danni per trattamento illecito di dati personali (è competenza del tribunale ordinario) e nemmeno emettere sanzioni penali.

Il Garante può agire per segnalazioni, reclami, ricorsi o indagini.

Durante le ispezioni il Garante chiede:

- l'informativa
- i documenti che riportano i consensi
- chi sono gli incaricati e chi i responsabili
- le deleghe a incaricati e responsabili

2. PERSONE

Interessato
È la persona a cui si riferiscono i dati oggetto di trattamento. Può essere fisica o giuridica, o anche non riconosciuta, la definizione è da prendere in senso lato includendo anche ad esempio sindacati, partiti politici, gruppi religiosi, enti collettivi in generale..

Art 4 comma 1

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

Titolare
Il titolare è colui che tratta i dati personali di qualcuno. Per ogni caso di trattamento di dati personali c'è sempre un interessato (colui a cui appartengono i dati) e un titolare del trattamento, mentre possono non esserci responsabile ed incaricato. Il titolare non va designato da nessuno, esserlo è una situazione di fatto.

Art 4 comma 1

f) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

Può trattarsi di una persona fisica o giuridica, nel qual caso tipicamente agisce attraverso un suo legale rappresentante nei confronti dei terzi. Il Garante ha disposto che nell'ambito di una pubblica amministrazione, una società o un ente, il titolare deve considerarsi la struttura nel suo complesso.
Il titolare è il soggetto che assume tutte le decisioni sul trattamento, ad esempio decide:

- quali dati trattare
- per quali finalità
- con quali modalità (es. cartacea o informatizzata)
- quali scelte fare sotto il profilo della sicurezza

Anche le persone comuni possono diventare facilmente titolari di trattamento: ad esempio ognuno è titolare del trattamento dei numeri di telefono nella rubrica del proprio cellulare.
Nel caso del social network Facebook, Facebook stesso è titolare del trattamento dei dati di tutti i suoi iscritti, e ognuno di essi è titolare del trattamento dei dati dei propri amici e delle persone di cui parla (che sono gli interessati). Prima di pubblicare un'immagine di qualcuno è necessario acquisire il consenso e fornire, anche oralmente, l'informativa.

Diversi soggetti possono essere contitolari di trattamento, quando assumono insieme le decisioni su un unico trattamento. Segue che dovranno agire congiuntamente anche per tutte le altre azioni: fornire l'informativa, o designare responsabili.
Quando invece più soggetti sono coinvolti nello stesso trattamento, ma ognuno di essi sceglie in modo autonomo le finalità e le modalità del trattamento, e come operare a riguardo della sicurezza dei dati, allora a ciascuno di essi si deve imputare la titolarità autonoma dei dati.

Il titolare può designare due figure subordinate a lui nel trattamento dei dati: responsabile e incaricato. Questo non lo libera però del tutto dalle sue responsabilità sul trattamento: il titolare mantiene la responsabilità di vigilare. Egli risponde sempre almeno per la vigilanza, il controllo e la scelta del responsabile. Deve verificare che il responsabile osservi le norme di legge e le istruzioni che gli sono state date con l'atto di nomina.

Responsabile

Art 4 comma 1

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

Art. 29. Responsabile del trattamento

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

Figura eventuale, che può essere facoltativamente designato dal titolare. Il responsabile può essere una persona fisica o giuridica preposto al trattamento dal titolare. Può essere interno alla realtà del titolare, o esterno (es. altra azienda). Il responsabile gode di una certa autonomia, organizzativa e decisionale, che distingue il suo ruolo da quello dell'incaricato (che non ha autonomia di sorta).

Il titolare può designare più responsabili, nel qual caso essi sono pari tra loro, dal momento che un responsabile non può designare un altro responsabile ma solo incaricati.

Questa catena molto semplice e corta crea nel pratico diversi problemi applicativi, perché spesso la realtà lavorativa non è altrettanto semplice e i rapporti non sono altrettanto corti. Inoltre mal si applica al caso di reti di enti, ciascuno dei quali è titolare autonomo di trattamento, ma che collaborano nel trattamento stesso.

Il titolare non può designare chiunque come responsabile, ma deve sceglierlo tra soggetti che per esperienza, capacità e affidabilità siano in grado di dare una idonea garanzia di rispettare le disposizioni in materia di trattamento e di sicurezza dello stesso.

La designazione deve essere fatta con atto scritto (per iscritto) di delega, ovvero un atto scritto il cui contenuto è la delega. Non deve essere firmata, in quanto non è un contratto; la firma vale solo come presa visione. La delega non deve necessariamente essere una designazione ad hoc, concretamente può essere una lettera o anche una clausola contrattuale, può far parte di un atto dal contenuto più ampio (es. il contratto). Non è necessario che sia nominativa, può riferirsi ad esempio alle funzioni svolte in un dato ufficio, essere genericamente rivolta a chi ricopre certi ruoli.

La delega deve essere dettagliata e specificare le istruzioni sul trattamento: la responsabilità del responsabile è relativa all'incarico conferitogli e dipende dal contenuto dell'atto. Il titolare ha l'obbligo di vigilare sul responsabile e accertarsi, anche con verifiche periodiche, che si attenga alle disposizioni di legge e alle istruzioni ricevute.

Il responsabile può essere interno o esterno alla struttura del titolare. Nel caso di un ente pubblico che affidi determinate attività a privati, il privato può assumere sia il ruolo di responsabile esterno sia di titolare autonomo.

Egli è un responsabile quando tratta dati nell'ambito di un'attività che ricade nella sfera di titolarità e di responsabilità del soggetto pubblico; in questo caso il privato è vincolato nel trattamento dalle stesse regole che vincolano il soggetto pubblico, ed è necessario un atto scritto

dell'amministrazione che deve indicare chi svolga il ruolo di responsabile.

Il privato è invece titolare autonomo quando si tratta di una figura distinta dall'amministrazione che decide autonomamente in base al trattamento, tratta i dati secondo quando previsto per i privati, e si assume di conseguenza ogni responsabilità.

Incaricato

Art 4 comma 1

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

Art. 30. Incaricati del trattamento

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.
2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

Figura eventuale. È necessariamente una persona fisica, che opera sotto la diretta autorità del titolare o del responsabile attenendosi alle istruzioni date.

Come per il responsabile, anche l'incaricato deve essere designato tale con atto iscritto che individui in modo preciso e puntuale l'ambito del trattamento, atto che individua la responsabilità dell'incaricato.

Chiunque tratti dati personali in una certa realtà deve essere designato incaricato dal titolare o dal responsabile con atto scritto. L'applicazione della legge si è mostrata rigorosa in questo senso: non solo i dipendenti di un azienda, ad esempio, ma chiunque anche solo guardi i dati personali anche se per un brevissimo periodo di tempo (es. uno stagista, un collaboratore, consulente) deve essere designato incaricato.

Questa applicazione rigorosa ha creato una problematica nella vita reale: chi non tratta i dati non deve venirci a contatto. Spesso, le aziende inseriscono nei contratti che stipulano con le società terze che potrebbero imbattersi nei dati (es. società di pulizia), queste inseriscono una clausola di integrazione del contratto relativa alla riservatezza: la società terza deve impegnarsi a non diffondere dai coi quali sia venuta casualmente in contatto durante l'espletamento delle sue funzioni. In questo modo l'azienda si tutela: nel caso che si abbia ad esempio una diffusione illecita di dati personali per causa dell'azienda terza, il titolare potrà agire per inadempimento nei confronti di questa.

3. PRINCIPI

Art. 11. Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:
   a) trattati in modo lecito e secondo correttezza;
   b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
   c) esatti e, se necessario, aggiornati;
   d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
   e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

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

Art. 3. Principio di necessità nel trattamento dei dati

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

Dai due articoli precedenti possono essere sintetizzati cinque principi da rispettare nella raccolta ed elaborazione dei dati personali.

- **PRINCIPIO DI LEICITA E CORRETTEZZA**

  i dati devono essere gestiti in modo lecito, ovvero conformemente alla legge, al Codice per la protezione dei dati personali, ai regolamenti e alla normativa comunitaria. Devono essere trattati in modo corretto ovvero conformemente al principio di buona fede e rispettare la trasparenza degli scopi perseguiti

- **PRINCIPIO DI FINALITA**

  il trattamento deve rispondere alle finalità individuate e rese note all'interessato da parte del titolare, che devono essere determinate, legittime e rese esplicite (es. con l'informativa). Questo principio assume particolare importanza per il trattamento di dato effettuato dai soggetti pubblici, i quali non devono chiedere il consenso per il trattamento, ma possono effettuarlo solo se necessario per lo svolgimento delle loro funzioni istituzionali.

- **PRINCIPIO DI NECESSITA**

  l'uso di dati personali deve essere ridotto al minimo, ed escluso quando le stesse finalità possono essere raggiunte con dati anonimi o con misure che consentano l'identificazione solo in caso di necessità (es. impiego di codici identificativi). L'identificazione dell'interessato deve inoltre essere possibile per un periodo di tempo non superiore a quello necessario per il raggiungimento degli scopi della raccolta, trascorso il quale i dati devono essere cancellati o trasformati in forma anonima garantendo così il diritto all'oblio. Principio mutuato dalla legge tedesca.

- **PRINCIPIO DI ESATTEZZA**

  il titolare deve verificare che i dati trattati siano esatti, cioè veritieri e completi, così da garantire che essi rispecchino in modo fedele l'identità dell'interessato che non si vedrà rappresentato in modo falso e non sarà oggetto quindi di conseguenze

pregiudizievoli erronee. L'interessato ha il diritto di chiedere l'aggiornamento e la rettifica dei dati che lo riguardano, e quando ne ha interesse, anche l'integrazione. Ciò nonostante, il principio di esattezza deve essere rispettato a prescindere dalle richieste dell'interessato di operare sui dati.

- **PRINCIPIO DI PERTINENZA E NON ECCEDENZA**

  devono essere registrati ed elaborati solo i dati strettamente necessari per conseguire le finalità che sono state rese note all'interessato mediante l'informativa. I dati devono essere sufficienti a perseguire le finalità ma non devono essere eccedenti. È responsabilità del titolare compiere verifiche periodiche e sistematiche sulla strumentalità delle operazioni rispetto alle finalità. I dati eccedenti devono essere distrutti o resi anonimi.

4. INFORMATIVA

L'informativa è lo strumento fondamentale per assicurare il diritto alla protezione dei dati personali, è l'elemento di base per l'esercizio del diritto di controllo garantito dalla 196/03.

È un documento che informa l'interessato riguardo a chi detiene i suoi dati, come e per quali scopi.

L'informativa è dovuta dai titolari agli interessati sempre, è un adempimento generale che prevedere pochissime eccezioni.

Art. 13. Informativa

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

a) le finalità e le modalità del trattamento cui sono destinati i dati;

b) la natura obbligatoria o facoltativa del conferimento dei dati;

c) le conseguenze di un eventuale rifiuto di rispondere;

d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

e) i diritti di cui all'articolo 7;

f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

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

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

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

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

b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede

giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

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

L'informativa è un documento in cui è indicato

a) a cosa servono i dati raccolti e come vengono trattati (es. modalità cartacee, o piuttosto informatizzate)

b) i dati non necessari possono essere ammessi, altri no

c) ci sono casi in cui non si può concludere il servizio senza la fornitura dei dati

f) chi tratta i dati

L'informativa deve precedere, e non seguire, la raccolta dei dati.

Queste informazioni devono essere sempre fornite. La forma in cui sono fornite non è importante, essa può essere anche molto informale. Può essere anche molto sintetica, e non fornire elementi già noti all'interessato.

L'informativa può anche essere orale, e naturalmente non necessita di una firma.

La mancata fornitura dell'informativa comporta una sanzione amministrativa, ovvero una multa erogata dall'autorità amministrativa, in questo caso il Garante.

Art. 161. Omessa o inidonea informativa all'interessato

1. La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da seimila euro a trentaseimila euro.

La sanzione amministrativa per omessa o inidonea informativa va dai seimila ai diciottomila euro, con la possibilità, arrivando a trentamila euro nel caso che il trattamento riguardasse dati giudiziari o sensibili.

5. NOTIFICAZIONE DEL TRATTAMENTO

Art. 37. Notificazione del trattamento

1. Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:
   a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
   b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
   c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
   d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
   e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
   f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti fraudolenti.
2. Il Garante può individuare altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali, con proprio provvedimento adottato anche ai sensi dell'articolo 17. Con analogo provvedimento pubblicato sulla Gazzetta ufficiale della Repubblica italiana il Garante può anche individuare, nell'ambito dei trattamenti di cui al comma 1, eventuali trattamenti non suscettibili di recare detto pregiudizio e pertanto sottratti all'obbligo di notificazione.
3. La notificazione è effettuata con unico atto anche quando il trattamento comporta il trasferimento all'estero dei dati.
4. Il Garante inserisce le notificazioni ricevute in un registro dei trattamenti accessibile a chiunque e determina le modalità per la sua consultazione gratuita per via telematica, anche mediante convenzioni con soggetti pubblici o presso il proprio Ufficio. Le notizie accessibili tramite la consultazione del registro possono essere trattate per esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali.

La notificazione del trattamento è una comunicazione da effettuare al Garante prima di procedere a specifiche operazioni di trattamento, come ad esempio quelle su dati genetici, biometrici o

geografici, o attività di profilazione a fini commerciali o di selezione del personale.

La notificazione va effettuata una sola volta a prescindere dal numero di operazioni di trattamento e dalla durata del trattamento, attraverso l'apposito modulo predisposto dal Garante. La notificazione può riguardare anche più trattamenti con finalità correlate.

L'Art. 38 stabilisce le modalità per una valida e corretta notificazione, che deve essere effettuata col modulo apposito e trasmessa telematicamente.

L'elenco delle operazioni di trattamento con obbligo di preventiva notifica, perché potenzialmente dannosi e lesivi di diritti, può essere ampliato dal Garante con provvedimento ad hoc.

Sono previste sanzioni amministrative per la sanzione non effettuata, effettuata in ritardo, o incompleta. Una sanzione penale è prevista per una sanzione che riporti notizie false, ai sensi dell'Art. 168.

Art. 163. Omessa o incompleta notificazione

Chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro e con la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.

6. PRESUPPOSTI DI LEICITA DEL TRATTAMENTO

I presupposti di leicità di trattamento, ovvero le condizioni alle quali si possono trattare dati personali in modo lecito, sono del tutto diversi a seconda della natura giuridica del titolare del trattamento. Anche se il trattamento è sugli stessi dati sugli stessi dati, ciò che rileva non è il dato trattato ma solo la natura giuridica di chi tratta.

L'informativa deve essere fornita all'interessato in entrambi i casi..

6.1 PRESUPPOSTI DI LEICITA PER SOGGETTI PRIVATI

I soggetti privati (persone fisiche o giuridiche) possono trattare dati solo col consenso dell'interessato. Il presupposto di leicità è il consenso.

Art. 23. Consenso

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

Dare il consenso significa acconsentire al trattamento: si tratta di una dichiarazione di volontà. Il consenso deve essere espresso, deve essere dichiarato. Non si può presumere che il consenso sia stato dato, esso non può essere tacito o implicito.

La forma prevista per il consenso è molto libera, ad esempio il consenso può essere espresso in forma orale, col solo vincolo che esso deve essere documentato per iscritto.

La verbalizzazione è a carico di chi riceve il consenso, ed è necessaria come forma per la prova (rappresenta una prova pre-costituita).

Ad esempio sono validi i consensi al trattamento dei dati nelle interviste telefoniche espressi oralmente attraverso il mezzo del telefono, è sufficiente che l'intervistatrice annoti che in una certa data e orario una determinata persona ha espresso il suo consenso all'intervista.

Nel caso di trattamento di dati sensibili il consenso deve essere scritto. In questo caso la forma scritta è richiesta per la validità e non per la prova.

Per via telematica è possibile ottenere un consenso scritto. Il documento informatico è idoneo a integrare la forma scritta a fini informativa.

Il consenso (per soggetti privati) deve essere

- espresso (dichiarato, manifestato, non implicito o tacito)
- libero (ovvero liberamente espresso, non forzato, non obbligato, non minacciato, non espresso in stato di incapacità)
- scritto se si tratta di dati sensibili, documentato per iscritto se dati non sensibili
- informato (deve essere fornita l'informativa)
- specifico (riferito al trattamento specifico, specificato nell'informativa)
  se il consenso richiesto è per due trattamenti, esso non è più specifico

In sintesi, le caratteristiche del consenso sono: libero, espresso, informato, documentato per iscritto, specifico/determinato.

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

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

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

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

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

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

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

f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

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

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

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

archivi privati.

Esistono casi nei quali il consenso al trattamento non è richiesto (sempre ovviamente nel caso dei soggetti privati, in quanto i pubblici non chiedono mai il consenso).

Le eccezioni al consenso non sono eccezioni all'informativa. L'informativa va fornita ugualmente.

Alcuni casi:

- serve per adempiere a un obbligo di legge (es. nel lavoro subordinato al dipendente deve essere fornita l'informativa ma non deve essere chiesto il consenso).
- quando il consenso è necessario per la conclusione di un contratto (es, devo avere un indirizzo a cui recapitare quanto il cliente ha acquistato da me, in altre parole si tratta dei casi in cui non posso fare altrimenti)
- se si tratta di un dato pubblico, reso pubblico proprio per le finalità per cui lo voglio utilizzare (es. i professori hanno una pagina pubblica con l'email universitaria: questo dato pubblico può essere utilizzato senza chiedere il consenso ma non può essere utilizzato a piacere, deve essere utilizzato sempre per il fine per il quale è stato fornito, nei limiti e nel rispetto delle finalità per le quali è stato pubblicato, che in questo caso sarà la comunicazione con gli studenti, non può essere utilizzato ad esempio per l'invio di materiale pubblicitario)
- è necessario per investigazioni difensive, per far valere un diritto. Questo tipo di investigazioni sono normalmente svolte da un avvocato/legale di parte, o dall'interessato stesso. I dati raccolti devono essere utilizzati sono entro questa finalità e solo per il tempo necessario. (es. genitore con figlio a carico chiede all'università di avere il curriculum del figlio fuori corso -informazione amministrativa-. Se motiva questa sua richiesta con la necessità di far valere un suo diritto, può ottenerlo).

Art. 26. Garanzie per i dati sensibili

1. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti.
2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.
3. Il comma 1 non si applica al trattamento:
   a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;
   b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria.
4. I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:
   a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;
   b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;
   c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n.397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati

esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

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

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

Per i soggetti privati, trattare dati sensibili è possibile chiedendo un consenso scritto, previa informativa e previa autorizzazione del Garante. Il consenso scritto in questo caso è necessario per la validità stessa, non per la prova; per ottenerlo telematicamente serve un documento con firma digitale.

L'autorizzazione del Garante non deve essere richiesta caso per caso: il Garante emette un provvedimento generale con cadenza annuale, che viene pubblicato sulla Gazzetta ufficiale, dove sono indicati i dati e i trattamenti ammessi, raggruppati per ambiti specifici,.

Vi sono eccezioni alla richiesta del consenso anche per il trattamento dei dati sensibili. Si tratta di un elenco molto più breve rispetto a quello delle eccezioni per dati non sensibili.

Non è richiesto il consenso per il trattamento di dati sensibili

- da parte di associazioni politiche, religiose o filosofiche che trattino i dati dei loro membri (purché forniscano l'informativa, agiscano nelle finalità dichiarate, e non diffondano i dati).
- quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di qualcuno
- quando il trattamento è necessario per investigazioni difensive per far valere un diritto, che deve essere di rango pari a quello alla protezione dei dati personali (ovvero un altro diritto della personalità).
- quando è necessario per adempiere a obblighi di legge.

6.2 PRESUPPOSTI DI LEICITA PER SOGGETTI PUBBLICI

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

1. Le disposizioni del presente capo riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici.
2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.
3. Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.
4. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato.
5. Si osservano le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione.

I soggetti pubblici non devono chiedere il consenso per il trattamento, ma possono effettuarlo solo se questo è previsto da una norma di legge o per fini istituzionali. Il presupposto di leicità del trattamento è la funzione istituzionale del soggetto.

Ad esempio, l'università pubblica ha la funzione istituzionale di portare gli studenti al massimo grado di istruzione: può trattare tutti i dati che ritiene necessari per conseguire questo fine, ma non può trattare alcun dato per altra finalità.

La funzione istituzionale di un soggetto pubblico si trova scritta in qualche atto, tipicamente nello statuto dell'ente, in generale in leggi o regolamenti. L'espressione “funzione istituzionale” può essere interpretata sia in senso restrittivo (sono leciti solo i trattamenti necessari per l'espletamento dei compiti dell'ente) sia in senso estensivo (sono leciti anche i trattamenti volti a velocizzare o agevolare la realizzazione degli interessi pubblici affidati all'amministrazione): il Garante può pronunciarsi a questo proposito.

Le ragioni per le quali gli enti pubblici non devono chiedere il consenso è una ragione ideologica. La prima legge del '96, che ha preceduto l'attuale legge del 2004, era figlia di un dibattito sulla privacy degli anni '70. In quel clima culturale lo stato era visto come la più grande minaccia per la privacy, per via della grande quantità di dati dei cittadini che possedeva, e di conseguenza si sentiva il bisogno di porre limitazioni forti per i soggetti pubblici. Il consenso chiesto da un soggetto forte è un consenso debole, si ritenne maggior tutela limitare il trattamento a ciò che si trova nelle leggi o nei regolamenti, nella prospettiva di controllare maggiormente gli enti pubblici.

Al giorni d'oggi questa visione è obsoleta: i soggetti pubblici possiedono molti dati spesso non sono in grado di aggregarli neanche quando sarebbe non solo concesso ma necessario, la maggior minaccia è divenuta il soggetto in grado di aggregare le informazioni che possiede, quindi tipicamente le grandi società nell'IT (Facebook, Microsoft, Google..).

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

1. Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.
2. La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata.
3. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

La comunicazione dei dati da parte di un soggetto pubblico a un altro soggetto pubblico può avvenire in due casi:

- se previsto da una disposizione normativa, senza particolari formalità
- se necessario per i fini istituzionali dell'uno o dell'altro e previa comunicazione al Garante. Il silenzio del Garante dopo 45 giorni vale come assenso.

La comunicazione di dati a un soggetto privato può invece essere effettuata solo se prevista da una disposizione di legge. Se non lo è, il solo modo per il soggetto di pubblico di effettuarla è cambiare lo suo statuto. Non giustifica ottenere il consenso dell'interessato poiché il consenso non ha alcuna valenza per i soggetti pubblici.

Il soggetto pubblico non può in alcun caso fare riferimento agli articoli 23 e 24 che riguardano i soli soggetti privati.

Il Garante ha ritenuto legittimanti per la comunicazione e la diffusione ad esempio i regolamenti delle università, gli statuti e i regolamenti degli enti locali, oltre naturalmente ai regolamenti delle amministrazioni centrali e della presidenza del Consiglio dei ministri. Non ha ritenuto idoneo il regolamento interno di un ente pubblico.

Art. 20. Principi applicabili al trattamento di dati sensibili

1. Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.
2. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo.
3. Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2.
4. L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente.

La pubblica amministrazione non chiede il consenso per il trattamento neanche nel caso di dati sensibili: è vincolata all'esistenza di una norma di legge che preveda il trattamento. Un regolamento in questo caso non è sufficiente.

La norma di legge deve essere analitica, e specificare gli scopi del trattamento, i dati oggetto del trattamento, e le operazioni.

Un esempio di norma analitica con scopi, dati e operazioni: l'università può trattare dati di salute degli studenti per fini di prevenzione solo in forma anonima, non può comunicarli né diffonderli.

Un simile norma di legge è molto rara. Se la legge prevede solo gli scopi del trattamento, non dati e operazioni, la PA può dotarsi di un regolamento per trattarli, autorizzato dal Garante prima dell'inizio del trattamento.

Il regolamento deve essere sintetico e indicare: le tipologie di informazioni sensibili e giudiziarie (i dati), le operazioni di trattamento, e descrivere anche sinteticamente la complessiva attività svolta dall'ente.

Il regolamento può essere modificato e riproposto se rifiutato dal Garante. Il Garante ha predisposto con alcuni enti dei regolamenti poi approvati in blocco.

Il soggetto pubblico deve verificare periodicamente l'esattezza e l'aggiornamento dei dati sensibili, la loro pertinenza e completezza, non eccedenza e necessità rispetto alle finalità perseguite, e distruggere i dati eccedenti, non pertinenti o non necessari.

La diffusione di questi dati è lecita solo se prevista da una espressa disposizione di legge: un regolamento non è più sufficiente.

7. DIRITTI DELL'INTERESSATO

L'interessato di un trattamento di dati personali del quale almeno una parte avviene in Italia ha il diritto di

- ricevere l'informativa
- agire per il controllo con le azioni specificate dall'Art. 7
  - conoscere i dati e averne comunicazione (averne copia) in forma intelligibile (comprensibile, banale in alcuni casi ma non in tutti, ad esempio nel caso che il dato si trovi in una banca dati cifrata). La comunicazione può avvenire con ogni mezzo, non necessariamente cartaceo.
  - sapere quali elaborazioni sono state fatte e a chi sono stati comunicati

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

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'origine dei dati personali;
   b) delle finalità e modalità del trattamento;
   c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
   e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il diritto di ottenere l'aggiornamento non c'è nel caso si tratti di dati di tipo valutativo o relativi a giudizi, opinioni o apprezzamenti di tipo soggettivo (es. non si può far correggere un verbale).

La cancellazione è un operazione di tipo retroattivo, diversa dall'opposizione al trattamento, e può essere richiesta se i dati sono trattati in violazione di legge, o se non sono più necessari o pertinenti rispetto al fine per il quale erano stati raccolti.

È facoltà dell'interessato anche opporsi al trattamento dei dati in due casi: per i cosiddetti motivi legittimi, che verranno esposti e valutati dal titolare di trattamento che poi deciderà (es. caso avvenuto alla facoltà di giurisprudenza: una ragazza vittima di stalking non desiderava che le informazioni su quando avrebbe sostenuto gli esami fossero esposte in quanto il suo persecutore avrebbe avuto modo di sapere dove lei si trovava e quando, e infastidirla), o quando il trattamento avviene per fini commerciali.

MODALITA DI ESERCIZIO DEI DIRITTO

I diritti dell'interessato sono esercitabili nei confronti di chiunque tutte le volte che l'interessato desidera (col solo vincolo che essa non possa essere ripetuta prima di novanta giorni in assenza di giustificati motivi), senza limiti di tempo e senza fornire alcuna motivazione. L'esercizio di questo diritto deve essere gratuito, un contributo spese può essere richiesto solo in alcuni casi indicati dal Garante con una delibera del 23 dicembre 2004.

La richiesta dell'interessato al titolare è priva di particolari formalità, può anche essere orale se ha per oggetto la richiesta di conferma dei dati o di informazioni sui dati. Deve essere annotata sinteticamente dall'incaricato, o dal responsabile.

Diverse forme di identificazione, dell'interessato da parte del titolare, si possono considerare valide, come la conoscenza personale o l'attestazione da parte di terzi, non vi è l'obbligo ad esempio di presentare la carta d'identità.

I diritti su dati personali di persone decedute possono essere esercitati da chi ha un interesse proprio, agisce a tutela dell'interessato o per ragioni familiari meritevoli di tutela.

La riposta dal titolare di trattamento è dovuta entro 15 giorni dalla richiesta, se questa non perviene entro il termine è possibile fare ricorso al Garante, che in breve tempo ordinerà al titolare di agire come richiesto dall'interessato. Se la richiesta non è riferita a un particolare trattamento o a specifici dati, allora si deve ritenere riguardante tutti i dati e tutti i trattamenti.

Se richiesto, i dati devono essere forniti in forma elettronica.

Il diritto di controllo garantito dal diritto alla protezione dei dati personali è uno strumento potentissimo, che rivela anche un potenziale uso strumentale.

AZIONI IN CASO DI VIOLAZIONE

Esistono due forme di tutela in caso di violazione nel trattamento di dati personali: amministrativa e giurisdizionale. Si può scegliere liberamente quale delle due strade adottare.

La via amministrativa consiste nel presentare ricorso al Garante, secondo quanto previsto dall'Art. 153. La richiesta al Garante non richiede particolari formalità, né l'assistenza di un avvocato. Il Garante può ordinare a un titolare di trattamento che non risponde alle richieste di dare all'interessato le informazioni che chiede, o di aggiornarle o cancellarle, e può dichiarare illecito un certo trattamento e sanzionarlo, e tipicamente risponde ai ricorsi presentatigli in tempi molti brevi. Tuttavia, liquida le spese legali/amministrative ma non l'eventuale danno subito.

Il tribunale è diverso dal Garante poiché ha anche la facoltà di liquidare il danno. L'interessato può rivolgere tutte le sue richieste direttamente al tribunale, ma dal momento che si tratta di una procedura molto lunga, una terza soluzione è avvalersi di entrambe le tutele, rivolgendosi prima al Garante e successivamente al tribunale per il solo risarcimento dei danni.

8. MISURE DI SICUREZZA

La sicurezza è un concetto importante nel trattamento dei dati personali. È un obbligo di legge, e il titolare risponde del trattamento dei dati anche "sotto il profilo della sicurezza".

La sicurezza è informatica, ma anche giuridica e organizzativa, è costituita dal complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali. Le misure di sicurezza devono essere adottate nel caso di trattamento informatizzato ma anche di trattamento con metodi tradizionali (saranno logicamente misure diverse).

Gli obblighi di sicurezza riguardano tutte e tre le figure coinvolte nel trattamento dei dati, titolare, responsabile e incaricato. Ognuno di essi risponderà a seconda delle misure che era tenuto ad adottare dipendentemente dal suo ruolo (e dal contenuto della sua delega).

Art. 31. 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.

I rischi maggiori, individuati dalla legge, per i dati sono:

- distruzione o perdita, anche accidentale
- accesso non autorizzato
- trattamento non consentito o non conforme alle finalità di raccolta

La sicurezza non è un mero fatto tecnico, ma si fonda sui concetti di custodia, controllo e analisi dei rischi. I dati devono essere custoditi e controllati durante l'intero ciclo del loro trattamento, dalla raccolta alla distruzione.

Gli obblighi di sicurezza sono obblighi dinamici: fanno riferimento al progresso tecnico, e alla natura dei dati. Devono essere costantemente adeguati, rivisti e aggiornati alla luce del progresso tecnologico, non si considerano adempiuti per il solo fatto di averli adempiuti in un certo momento storico per una certa istanza di trattamento.

Art 4 Definizioni comma 3

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

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

Art. 33. Misure minime

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

Art. 34. Trattamenti con strumenti elettronici

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

a) autenticazione informatica;

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

c) utilizzazione di un sistema di autorizzazione;

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

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

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

g) tenuta di un aggiornato documento programmatico sulla sicurezza;

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

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.

Alcune precisazioni su quanto richiesto dall'Art. 34 (considerando anche l'allegato B)

- Autenticazione: l'autenticazione può venire con un codice e una parola chiave riservata (classico username e password), o con altri mezzi, ad esempio con il riconoscimento di caratteristiche biometriche. Il codice (es. username) non può essere assegnato ad altri incaricati, neanche in tempi diversi. Le credenziali non utilizzate da almeno sei mesi devono essere disattivate. Le disposizioni sull'autenticazione non si applicano per trattamenti di dati destinati alla diffusione.
- Credenziali di autenticazione: valgono le solite regole per le password. Devono essere sufficientemente lunghe, non banali, difficilmente ricostruibili. Non sono ammesse password di gruppo. Ogni soggetto che possiede credenziali di autenticazioni è tenuto a tenerle segrete e ad adottare cautele per evitarne l'acquisizione da parte di terzi. Devono essere modificate di frequente, almeno ogni sei mesi se permettono l'accesso a dati comuni,

almeno ogni tre se a dati sensibili.

Le credenziali sono importanti anche perché permettono di imputare una responsabilità. Giuridicamente costituiscono prove.

Il cambio della password è necessario solo se si accede a dati di terzi: se noi accediamo con la nostra password ai nostri dati, ad esempio alla nostra email, non siamo tenuti per legge a cambiarla regolarmente (anche se è buona pratica), né è chi ci fornisce il servizio tenuto a chiederci di cambiarla.

- Autorizzazione: non tutti dovranno essere in grado di accedere agli stessi dati, secondo il principio di pertinenza e non eccedenza nessuno dovrà accedere a dati che non gli servono per il compito che dovrà svolgere.

  I soggetti autorizzati dal titolare o dal responsabile devono accedere solo ai dati necessari per lo svolgimento dei loro compiti, e svolgere su di essi solo le operazioni di trattamento necessarie. È necessario quindi individuare e configurare (anteriormente all'inizio del trattamento) dei profili di autorizzazione così da limitare l'accesso ai soli dati necessari per le operazioni di trattamento. I profili devono essere rivisti almeno annualmente, verificando la sussistenza delle condizioni per la loro conservazione.
- Misure per proteggere dati, elaboratori, programmi: devono essere adottate e aggiornate regolarmente, almeno semestralmente. Sono previsti anche programmi “contro il rischio di intrusione” e “volti a prevenire le vulnerabilità e a correggerne difetti”. In altre parole, si deve aggiornare l'intero sistema, si devono utilizzare firewall e antivirus, e anch'essi devono essere mantenuti aggiornati.
- Backup: deve essere almeno settimanale, e deve essere conservato in un ambiente separato e distante da dove si trovano i dati originali.
- Cifratura: è richiesta per il trasporto dei dati sulla salute o la vita sessuale (o solo i dati genetici?) in formato elettronico. Per gli altri trattamenti questo tipo di dati sensibili deve essere protetto, ma si può optare sia per la cifratura che per la separazione e l'utilizzo di codici.
- Supporti rimovibili: devono essere custoditi per evitare accessi illeciti, devono essere distrutti se non utilizzati. Possono essere riutilizzati solo se le informazioni che contenevano non sono più ricostruibili in alcun modo.
- Documento programmatico sulla sicurezza: deve essere adottato da coloro che trattano dati sensibili o giudiziari con mezzi informatici (due presupposti: natura dei dati trattati e modalità del trattamento). Costituisce una sorta di bilancio preventivo e consuntivo sulla sicurezza del trattamento, deve riassumere lo stato sia generale sia informatico della sicurezza del soggetto che tratta, determinare le azioni da intraprendere, individuare i rischi per i dati e le contromisure da adottare.

9. RESPONSABILITA PER DANNI DA TRATTAMENTO DI DATI PERSONALI

9.1 LE TRE RESPONSABILITA

Se le regole non sono rispettate il trattamento è illecito, e si possono configurare per il soggetto che compie l'illecito diverse responsabilità che vedremo.

Vediamo quindi prima i tre tipi di responsabilità:

- civile

  la responsabilità civile è la responsabilità che consegue dall'avere cagionato un danno. Si rimborsa, vi è l'obbligo di risarcire il danno dal danneggiante al danneggiato. Il danneggiato deve intraprendere un azione per ottenere il risarcimento.

  La responsabilità civile non deriva da contratto, bensì da "fatto illecito", e l'articolo che la regola è il 2043 del Codice Civile.

- amministrativa

  es. multe e contravvenzioni. È una responsabilità solo pecuniaria. Si prescinde dall'azione di un soggetto, l'autorità amministrativa agisce da sola su sua iniziativa, ha tutti i poteri.

- penale

  si ha in caso di violazioni della legge penale (reati: fatti puniti dalla legge penale, non si dice reato penale poiché il reato è sempre penale), e arriva fino a prevedere la pena più grave, la privazione della libertà ovvero la reclusione. Solo i fatti più gravi, come omicidio, lesioni personali, lesioni al diritto di proprietà, dovrebbero essere puniti dalla legge penale, ma ormai la legge si è estesa alla protezione di beni non primari, come ad esempio il diritto d'autore.

  La sensazione è di uno scollamento molto forte tra il sentire sociale e la sanzione penale. Le ragioni per le quali il legislatore ha scelto di sanzionare in modo molto severo fatti lievi sono da un lato la forte azione delle lobby di settore, dall'altro l'ineffettività delle altre sanzioni, che si sono volute inasprire data la loro incapacità di fungere da deterrente.

9.2 RESPONSABILITA DELLA SICUREZZA

Vi sono due livelli di sicurezza: il livello minimo, che consiste nell'adozione delle misure minime di cui all'Art. 33, e quello costituito da "tutte le misure idonee ad evitare il danno" (Art. 2050 Codice Civile).

Il titolare del trattamento ha tutte e tre le responsabilità, penale, civile e amministrativa.

Responsabilità penale

Il requisito per evitare la responsabilità penale: si devono adottare le misure minime di sicurezza, che sono misure precise ed elencate, il cui costo di adozione è quindi chiaramente quantificabile.

Le misure minime di sicurezza si trovano nel Codice (es. Art 34), ma devono anche essere integrate con quanto disposto dal disciplinare tecnico di cui all'Allegato B del Codice.

La loro mancata adozione genera conseguenze di natura penale secondo l'Art. 169. Chi è tenuto ad adottare le misure minime, e paga quindi con la reclusione?

Chiunque "essendovi tenuto", quindi potenzialmente tutti i soggetti coinvolti, titolare, responsabile e incaricato, ma in modo diverso: ognuno risponde penalmente per il comportamento che era tenuto ad avere, a seconda delle proprie competenze e del proprio ruolo.

Responsabilità amministrativa

La non adozione delle misure minime di sicurezza dell'allegato B porta anche a una sanzione amministrativa, secondo l'Art 162 comma 2bis, che è la più temuta in quanto è immediata (non serve un processo) e si può avere anche senza che alcun danno vi sia stato. Il presupposto per la sanzione amministrativa infatti non è l'aver cagionato un danno, ma il non aver adottato le misure di sicurezza. La sanzione amministrativa è di recente introduzione, e varia da 20mila a 120mila euro. Può essere impugnata se ritenuta ingiusta o eccessiva.

Responsabilità civile

Su un livello completamente diverso è invece il requisito per evitare la responsabilità civile.

L'adozione delle misure minime di sicurezza non è sufficiente a evitare la responsabilità civile, per evitarla si deve provare che si è evitato il danno con tutte le precauzioni adeguate secondo lo stato dell'arte.

Le misure da adottare saranno quindi da individuare di volta in volta, e cambieranno nel tempo. La loro adozione corretta ha potenzialmente un costo altissimo.

Se qualcuno è danneggiato da una mancanza di misure di sicurezza si cade nell'Art. 15, "Danni cagionati per effetto del trattamento".

9.3 IL RISARCIMENTO DEL DANNO PER EFFETTO DEL TRATTAMENTO

Art. 15. Danni cagionati per effetto del trattamento

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

Art. 2050 CC 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, e tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.

Art. 2043 CC Risarcimento per fatto illecito

Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno.

Infatti, i danni causati dal trattamento dei dati personali generano la stessa responsabilità civile dei danni causato dall'esercizio di attività pericolose di cui all'Art. 2050 CC. La responsabilità civile dell'Art. 2050 CC (eccezione alla responsabilità del 2043, responsabilità per fatto illecito in generale) è una responsabilità oggettiva, nel senso che non è necessario dimostrare il dolo o la colpa di chi ha causato il danno(elementi soggettivi), ma solo i tre elementi oggettivi di danno, fatto, e nesso di causalità tra i due. L'unica prova ammessa dal 2050 per liberarsi della responsabilità del danno è dimostrare di aver adottato tutte le precauzioni di sicurezza per evitare il danno.

Si tratta di una prova liberatoria difficilissima da fornire, che si riduce alla prova del caso fortuito, ovvero la situazione che non poteva in alcun modo essere prevista e quindi evitata.

L'Art. 2050 inverte l'onere della prova: mentre l'Art. 2043 CC (la norma generale per la risarcibilità del danno causato da fatto illecito) stabilisce che il danneggiato è tenuto a provare di avere diritto al risarcimento portando tutte le prove, ovvero dimostrando danno, fatto, nesso di causalità e dolo o colpa del danneggiante, nel 2050 il danneggiato deve provare solo i primi tre elementi (relativamente semplici), e la prova di reale difficoltà deve portarla il danneggiante.

Non hanno quindi rilevanza il dolo del danneggiante, e nemmeno la colpa (e quindi la perizia o la prudenza usate o non usate).

L'Art. 2050 tutela moltissimo il danneggiato, configurando la responsabilità civile più severa prevista da Codice Civile.

La direttiva comunitaria 95/46/CE dispone che le misure di sicurezza “devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere”. Uno dei criteri di valutazione deve essere dunque costituito dai costi economici delle misure di sicurezza. La legge italiana si discosta dalla direttiva europea: la valutazione dell'impatto economico è del tutto assente.

Una sentenza in merito: Orvieto, 2000. Due coniugi commercianti si rivolsero alla banca di Orvieto, la quale aprì un indagine sui due per conoscere, oltre allo stato delle loro finanze, la loro reputazione.

Un'amica della coppia si recò in banca per suoi motivi, e le capitò di aver modo di vedere il contenuto del fascicolo sui coniugi, che era stato lasciato aperto e incustodito in un ufficio. Il fascicolo conteneva informazioni vere ma molto negative, e la coppia chiese alla banca un risarcimento dei danni alla reputazione causati da trattamento non conforme di dati personali, che ottenne, per l'ammontare di 50mila euro.

Il fatto era stato provato dalla testimone, il nesso di causalità e il danno alla reputazione erano

immediati, e, secondo quanto stabilito dall'Art. 15 e conseguentemente dall'Art. 2050 CC, i coniugi non dovevano provare altro. La banca non riuscì a portare la prova liberatoria richiesta, in quanto è evidente che quello non era il modo di conservare un fascicolo.

(Se le informazioni nel fascicolo fossero state positive il trattamento sarebbe stato comunque non adeguato, ma sarebbe stato più difficile per i coniugi provare di aver subito un danno.)

Se viene violato l'articolo 11 è possibile chiedere il risarcimento anche per danni non patrimoniali, chiedere cioé un risarcimento delle sofferenze fisiche o psichiche del danneggiato. L'articolo 11 dà principi generali sulle modalità del trattamento e sui requistii dei dati, che devono essere trattati lecitamente e secondo correttezza, osservando il principio di finalità, di necessità, completezza, esattezza, pertinenza e non eccedenza.

Il danno non patrimoniale può essere risarcito solo nei casi previsti dalla legge (come questo).

Art. 1226 CC Valutazione equitativa del danno

> Se il danno non può essere provato nel suo preciso ammontare, è liquidato dal giudice con valutazione equitativa (2056 e seguenti).

In altre parole, il giudice decide discrezionalmente, senza alcun vincolo, facendo riferimento ai criteri equitativi di cui all'Art 1226 CC, l'entità della liquidazione per danni non patrimoniali, diversamente da quanto accade per i danni fisici, per i quali ormai sono state definite tabelle a cui i giudici tipicamente fanno riferimento.

Una seconda sentenza di rilievo è quella che liquidò, a una signora che aveva fatto ricorso per messaggi telefonici pubblicitari indesiderati, la somma di mille euro per ogni messaggio ricevuto.

L'ammontare del danno per effetto del trattamento di dati personali non è preventivamente quantificabile, o lo è difficilmente, e infatti non vi sono assicurazioni che coprano questo tipo di rischio.

Spesso, gli illeciti in materia di trattamento di dati personali danno origine a una catena di responsabilità: un'azienda può agire per inadempimento su un responsabile esterno, e chiedere il risarcimento del danno di lesione del diritto all'immagine. La Corte di Cassazione, con una pronuncia del 2006, ha ritenuto legittimo il licenziamento del dipendente che ha rivelato a un terzo estraneo all'azienda la propria password di accesso alla rete aziendale, come sanzione proporzionale alla gravità della mancanza del lavoratore.

10. SANZIONI

10.1 VIOLAZIONI AMMINISTRATIVE

Sono previste sanzioni amministrative per:
- omessa o inidonea informativa (Art. 161)
- mancata adozione delle misure minime di sicurezza (Art. 162 comma 2 bis, anche penale)
- omessa o incompleta notificazione (Art. 163)
- omessa informazione o esibizione al Garante (Art. 164)
- ...

10.2 ILLECITI PENALI

Costituiscono reati:
- trattamento illecito (Art. 167)
- false dichiarazioni al Garante (Art. 168, fino a tre anni)
- mancata adozione delle misure minime di sicurezza (Art. 169, fino a due anni e sanzione amministrativa)
- inosservanza di provvedimenti del Garante (Art. 170, fino a due anni)

Art. 167. Trattamento illecito di dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

Perché vi sia questo reato devono verificarsi tre condizioni:
- trattamento illecito (es. per finalità diverse da quelle istituzionali o dichiarate..)
- fine di profitto o danno (dolo o profitto)
- effettivo nocumento (danno che si è effettivamente avuto)

Es. vendita di dati personali da parte di una banca
- illecità: vendita non consentita
- dolo: il profitto
- danno: lesione al diritto alla protezione dei dati personali

Anche lo spamming rientra qui: riservatezza e protezione dei dati personali lesa.

Il primo comma si riferisce alle violazioni riguardo mancanza dei presupposti di leicità per soggetti pubblici (Art. 18, 19), privati (Art. 23), dati su traffico (123) e ubicazione (126), comunicazioni indesiderate (130).

Nel secondo comma 2 (sanzione più grave) il riferimento è al trattamento che prevede rischi (17), trattamento di dati sensibili e giudiziari, comunicazione e diffusione (20, 21, 22, 25, 26, 27), trasferimenti all'estero vietati (45).

Art. 168. Falsità nelle dichiarazioni e notificazioni al Garante

Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

Art. 170. Inosservanza di provvedimenti del Garante

Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni.

Esempi di provvedimenti del Garante: quello sul controllo della posta elettronica dei lavoratori, quello sugli amministratori di sistema.

Nel 2007 l'On. Sircana era stato coinvolto in uno scandalo a seguito di un intercettazione telefonica in cui un fotografo parlò di una sua fotografia compromettente in cui parlava con un transessuale. Il Garante ne vietò la pubblicazione con un provvedimento in cui vietava di diffondere notizie le quali “si riferiscano a fatti e condotte private che non hanno interesse pubblico”. In quel caso appunto, la non osservazione del provvedimento avrebbe portato alla violazione dell'Art. 170.

11. LA TUTELA CAUTELARE

Art. 700 CPC Condizioni per la concessione (dei provvedimenti d'urgenza)

> Fuori dei casi regolati nelle precedenti sezioni di questo capo, chi ha fondato motivo di temere che durante il tempo occorrente per far valere il suo diritto in via ordinaria, questo sia minacciato da un pregiudizio imminente e irreparabile, può chiedere con ricorso al giudice i provvedimenti d'urgenza, che appaiono, secondo le circostanze, più idonei ad assicurare provvisoriamente gli effetti della decisione sul merito.

La tutela cautelare è un provvedimento d'urgenza che si può richiedere quando c'è il pericolo fondato di temere che prima di giungere al processo che farà valere il diritto, il soggetto sia minacciato o leso. Esempi di tutela cautelare sono il ritiro di riviste dal commercio, o l'oscuramento di siti o cartelli pubblicitari.

In prima battuta si tutela quindi il soggetto apparentemente leso, poi ci sarà il processo in cui il giudice dovrà accertare sia davvero una lesione del diritto, e emetterà una decisione detta di merito.

Il provvedimento della tutela cautelare è provvisorio, i suoi effetti si esauriscono con il provvedimento di merito. I provvedimenti cautelari non sono mai fini a se stessi, ma sono al servizio del provvedimento definitivo, sono rivolti ad evitare i danni che potrebbero esserci nel tempo necessario allo svolgimento del processo e al raggiungimento della sentenza definitiva.

Le condizioni per richiedere la tutela cautelare sono due:

- fumus boni iuri

  “apparenza di buon diritto”. Deve sembrare a un esame preliminare che il diritto vantato ci sia realmente, deve essere verosimile.

- pericolum in mora

  pericolo nel ritardo. Pericolo da infruttuosità (si teme che al momento del processo non si sarà più in grado di emettere un provvedimento fruttuoso se si aspetta) o pericolo da tardività dell'intervento (si anticipano gli effetti del provvedimento definitivo per evitare che questo sia inefficace in quanto giunto troppo tardi.).

La tutela cautelare è importante perché garantisce l'effettività della tutela giurisdizionale. Negli articoli 7 e 10 del Codice (tutela del diritto al nome e all'immagine) è prevista la possibilità di una tutela preventiva con un'azione inibitoria il cui contenuto è l'ordine di cessazione del fatto lesivo, dell'abuso.

12. TRASFERIMENTI DI DATI ALL'ESTERO

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

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

I dati personali possono circolare liberamente nei paesi membri dell'Unione, che hanno tutti la stessa normativa in materia di protezione di dati personali. È possibile introdurre provvedimenti per evitare che in qualche modo i trasferimenti siano fatti per sfuggire alle norme.

I paesi dell'Unione hanno da diverso tempo una normativa in materia di protezione dei dati personali, in quanto averla era condizione per aderire all'accordo di Schengen operativo dal 1995. Questo accordo è lo stesso che spinse l'Italia a dotarsi di una legge in materia.

Nella relazione annuale del 2006 del Garante per la protezione dei dati personali è stato dato ampio spazio alle cosiddette ***Binding Corporate Rules***, ovvero le regole per l'impresa che voglia trasferire dati personali in paesi non appartenenti all'Unione Europea.

Art. 43. Trasferimenti consentiti in Paesi terzi

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

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

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

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

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

e) è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

f) è effettuato in accoglimento di una richiesta di accesso ai

documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia;

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

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

Art. 44. Altri trasferimenti consentiti

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

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

b) individuate con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, con le quali la Commissione europea constata che un Paese non appartenente all'Unione europea garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti.

Sono consentiti alcuni trasferimenti alle condizioni dell'Art. 43, ad esempio che l'interessato abbia prestato il suo consenso espresso, o che il trasferimento sia necessario, per adempiere a un obbligo di legge, per la salvaguardia della vita, per investigazioni difensive.

È comunque possibile trasferire dati in altri casi (Art. 44), autorizzati dal Garante, che li consentirà se vi saranno adeguate garanzie per l'interessato. Le garanzie potranno trovarsi in contratti o regole di condotta, o anche in decisioni europee.

A questo riguardo, per il trasferimento di dati verso gli Stati Uniti, esiste l'accordo Safe Harbor ("approdo sicuro"). È un accordo su sette principi di protezione dei dati personali nato nel 2000 tra le autorità europee e quelle statunitensi.

Rivolto alle aziende che trattano dati personali, negli Stati Uniti ha carattere facoltativo, ovvero può essere liberamente sottoscritto o meno. Il controllo sulle aziende statunitensi che sottoscrivono l'accordo, e devono quindi trattare i dati provenienti dall'Unione Europea secondo i principi del Safe Harbor, è effettuato dalla Federal Trade Commission (USA).

La sottoscrizione dell'accordo permette alle aziende o multinazionali di trasferire i dati senza limitazioni e senza rischiare interventi europei di congelamento dei dati.

I sette principi sono estratti dalla direttiva europea 95/46/Ce e sono:

- informativa agli interessati
- consenso esplicito per i dati sensibili

- consenso implicito per i dati non sensibili
- facoltà di accesso ai dati
- rispetto delle regole minime di sicurezza dei dati
- attuazione del principio di finalità, secondo cui i dati non possono essere trattati per fini diversi da quelli per cui sono raccolti
- attuazione del principio di pertinenza, secondo cui i dati devono essere funzionali agli scopi per i quali sono stati raccolti.

LA POSTA ELETTRONICA DEL DIPENDENTE

A chi appartiene la posta elettronica del dipendente? Il datore di lavoro può controllarla?

La posta elettronica del dipendente è un dato personale, se il dipendente ha ricevuto l'informativa e ha prestato il proprio consenso il datore di lavoro potrà fare dei controlli a campione e in forma anonima. Per effettuare controlli ci sono una serie di step che il datore di lavoro potrà fare, a determinate condizioni.

Controlli continui e di massa sono vietati dallo statuto del lavoratori, e sono altresì vietati controlli per verificare il lavoro del dipendente.

Il Garante per la privacy si è espresso su questo argomento con uno specifico provvedimento.

Un caso che ha segnato la giurisprudenza è stato al tribunale di Milano: un datore di lavoro era entrato nella posta elettronica lavorativa di una dipendente durante una sua assenza (per malattia o vacanza) e aveva scoperto che ella lavorava per la concorrenza. La lavoratrice era stata licenziata ed aveva citato il datore di lavoro: il Tribunale stabilì che la posta elettronica è sì strumento di lavoro ma è anche personale, e quindi il datore di lavoro aveva avuto torto nell'accedervi.

Ora, un caso del genere non potrebbe più accadere in questi termini: secondo il provvedimento del Garante, ogni luogo di lavoro deve avere una policy sulla privacy, il datore di lavoro non può accedere alla posta del lavoratore ma il lavoratore deve assicurarsi che in sua assenza le sue comunicazioni di tipo lavorativo siano accedibili, ad esempio designando per l'accesso un collega fidato. È anche buona norma, scrive il Garante, predisporre indirizzi email lavorativi a carattere collettivo, e allegare alle mail una firma che indichi che quell'indirizzo non è confidenziale.

La riservatezza della propria casella di posta personale è invece tutelata senza eccezioni dall'Art. 15 della Costituzione.