

Lezione 1

Se nel suo lavoro un dipendente, anche episodicamente, deve visionare o utilizzare documenti riguardanti dati personali di qualcuno, deve sapere che ora ci sono regole nuove e importanti da rispettare. Perciò è necessario che le conosca almeno a grandi linee, in modo da evitare errori che potrebbero causare problemi alla struttura in cui è inserito. La breve panoramica offerta in queste pagine consentirà di comprendere la nuova situazione e di collaborare consapevolmente con i colleghi che hanno maggiori responsabilità nella gestione dei dati personali.

Le nuove regole sono contenute nel Decreto Legislativo del 30 giugno 2003, n. 196, denominato “Codice in materia di protezione dei dati personali”. Per brevità d’ora in poi lo chiameremo semplicemente “Codice Privacy”. E’ il Testo Unico che ha sostituito con un unico atto normativo la legge 675 del 1996 sulla privacy e decine di altre leggi sull’argomento che avevano creato una complessa giungla normativa. Però ha anche introdotto parecchie novità.

Il breve compendio che state per leggere **non tratta la normativa per tutti, bensì soltanto quella specifica per gli enti pubblici non economici** (esempio: **Scuola Pubblica, Comuni, Province, Regioni, Agenzie ed organi statali, etc; gli Organismi Sanitari Pubblici hanno regole speciali in quanto trattano dati particolarmente protetti: per loro esiste un apposito manuale, parzialmente differente dal presente**).

Nasce un nuovo diritto del Cittadino: il Diritto alla protezione dei suoi dati personali

La prima regola del Codice Privacy è: “Chiunque ha diritto alla protezione dei dati personali che lo riguardano. Il presente testo unico garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell’interessato, con particolare riferimento alla riservatezza, all’identità personale e al diritto alla protezione dei dati personali. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà”. Quindi **il nuovo Codice Privacy non persegue solo la difesa della privacy, ma anche la protezione dei dati personali e introduce il diritto di ciascuno a controllare quasi completamente l’uso che gli altri possono fare di tutte le informazioni che lo riguardano**. Il «diritto alla protezione dei dati personali» quale prerogativa fondamentale della persona, è stato sancito in attuazione dell’art. 8 della Carta dei Diritti Fondamentali dell’Unione Europea del 7 dicembre 2000 e **deve considerarsi quale diritto nuovo rispetto al diritto alla riservatezza**.

Mentre il rispetto della riservatezza è un’idea ormai universalmente conosciuta, la protezione dei dati personali è un concetto nuovissimo. Significa che ogni cittadino ha diritto di conoscere e controllare la circolazione delle informazioni che lo riguardano. Perciò **qualsiasi Ente pubblico o ditta privata o associazione etc. può utilizzare informazioni o dati su un cittadino solo rispettando queste condizioni:**

- **prima di cominciare ad usarli deve informare il cittadino stesso degli scopi**

esatti per cui li chiede, delle modalità con cui li tratterà e a chi li comunicherà;

- i dati saranno usati esclusivamente per gli scopi dichiarati e solo per il tempo necessario a raggiungerli (e dopo dovranno essere distrutti);
- i dati saranno custoditi con la massima cura proteggendoli da furti, fughe di notizie e accessi non autorizzati di qualsiasi sorta;
- in qualsiasi momento, su richiesta del cittadino, deve mostrargli tutte le informazioni che detiene su di lui ed eliminarle o correggerle, se lui lo chiede.

E' come un contratto tra cittadino e Ente che utilizza il suo dato personale.

In sostanza **ogni informazione su se stesso il legittimo proprietario la affida momentaneamente in uso temporaneo** all'Ente o Ditta che la utilizza, **come se fosse un contratto**, quindi con condizioni chiare, per uno scopo dichiarato e precise regole da osservare. L'Ente o Ditta che ha temporaneamente in uso il dato risponde non solo della "fuga di notizie", ma anche del furto o della semplice perdita di tale dato. Inoltre, risponde se acquisisce il dato senza averne diritto, se lo comunica quando o a chi non è consentito o se lo trattiene quando il diritto di detenerlo è cessato. Infine, se il proprietario del dato vuol fare un'ispezione sul suo uso, deve essere accontentato in tempi rapidi. E' come quando dai un medaglione d'oro all'orafo perché vi incida una dedica: può detenerlo solo per quella finalità e solo finché non ha eseguito il lavoro, poi deve restituirlo; se lo perde o glielo rubano, ne risponde. Oppure è un po' come un conto in banca: il legittimo proprietario fa un deposito per un certo scopo e per un periodo limitato, ma quanto depositato resta suo; se venisse perduto, per qualsiasi ragione, la banca ne risponderebbe. Inoltre, come il titolare di un conto in banca in qualsiasi momento e a sua discrezione può verificarne l'importo, il legittimo proprietario dei dati ha il diritto in ogni momento di sapere quali sono esattamente i suoi dati personali detenuti da un terzo.

Le misure di protezione

In pratica questo significa che **oltre alle misure per garantire il riserbo su ogni dato personale, c'è l'obbligo di adottare adeguate misure per proteggere il dato** da furti, smarrimenti, distruzioni casuali ed accessi da parte di persone non autorizzate o con modalità improprie. Sono le cosiddette "**misure minime di sicurezza**", che devono assolutamente essere adottate da tutti, pena severe sanzioni penali e pecuniarie nonché la concreta possibilità di dover rispondere dei danni materiali e morali eventualmente causati.

Le nuove garanzie affinché ciascuno resti padrone dei propri dati

A presidio di questo nuovo diritto sono state messe regole forti e sanzioni pesanti (multe, condanne penali e diritto di risarcimento civile quasi automatico per i danni materiali e morali).

In ogni caso, chi raccoglie dei dati deve prima dare all'interessato una chiara informativa che spiega a cosa servono i dati raccolti, come sono trattati, chi li conoscerà, chi ne risponde e come far valere in qualsiasi momento alcuni diritti di conoscenza sui dati posseduti e di eventuale cancellazione o modifica.

Gli enti pubblici hanno il limite che possono trattare i dati personali di chiunque solo per compiti istituzionali. Invece il privato ha il limite che deve ottenere il consenso preventivo dell'interessato per usare i suoi dati.

Se i dati sono delicati, deve esserci anche una legge o uno speciale provvedimento del Garante Privacy che autorizza il fatto stesso di raccogliarli o di utilizzarli.

Le uniche eccezioni a tutte queste regole sono quelle motivate da esigenze forti della collettività (difesa dello stato, sicurezza pubblica, emergenze, ecc.).

Il Garante Privacy

Per far rispettare il Codice Privacy è stata istituita un'apposita autorità garante, chiamata "Garante Privacy", che detiene il potere di dettare regole, di eseguire ispezioni e di irrogare pesantissime sanzioni. Il mancato rispetto del Codice Privacy può comportare anche reati penali connessi; in questo caso la competenza è della Magistratura. La Polizia Postale e la Guardia di Finanza hanno ricevuto l'incarico di verificare il rispetto delle regole: gran parte del loro personale ha seguito corsi di formazione sul Codice Privacy per fare i controlli.

COS'È UN DATO PERSONALE

Per "persona" s'intendono sia gli esseri umani che le persone giuridiche

Quando il Codice Privacy parla di "persona" intende sia la persona fisica che la persona giuridica (=Società, Enti, Associazioni): pertanto ogni informazione sulla Telecom, sul Comune di Milano o sul WWF è dato personale, e perciò rientra a pieno titolo nelle regole e misure protettive previste dal Codice Privacy.

Definizione di dato personale

Un dato personale è qualunque informazione relativa a persona fisica, persona giuridica, Ente od associazione, **identificati**. O **identificabili**, anche indirettamente, mediante riferimento a qualsiasi altra informazione. Analizziamo in dettaglio.

Il dato personale è un'informazione

Il dato personale è una qualsiasi informazione inserita in un documento cartaceo, elettronico o in un archivio/file informatico, ma può consistere anche in una foto, una registrazione audio o cine/video, una lastra radiografica, un'impronta digitale, lo schema del suo DNA, il testo di una valutazione sulla persona, etc. Va sottolineato che **costituisce "dato personale" qualunque informazione (e non solo quelle di carattere riservato o particolare).**

E' impossibile fare un elenco completo dei dati personali, perché sono innumerevoli. A titolo di esempio: dati anagrafici, nome e cognome, indirizzo, residenza anagrafica, indirizzo postale, indirizzo di posta elettronica, numero telefonico, codice fiscale, partita iva, codice sanitario, qualunque codice identificativo compreso bancomat e carta di credito, ecc.. Ma anche valutazioni, profili personali, abitudini, profili professionali, origini razziali, fede religiosa e opinioni sull'argomento, opinioni politiche, sindacali, stato di salute, hobbies, gusti gastronomici, preferenze in qualsiasi campo, inclinazioni sessuali, ecc.. E ancora: i numeri di telefono chiamati in un certo momento, il fatto stesso di aver eseguito una telefonata in quel momento, lo scontrino del supermercato, ma anche il fatto stesso di aver fatto la spesa al supermercato, il contenuto della mia pattumiera in quanto si può ricavare che cosa ho mangiato o utilizzato, e così via... I dati personali sono riferibili anche ad enti (sia pubblici che privati), associazioni, Ditte e società: denominazione sociale, sede, indirizzo, numero di telefono, indirizzo email, co-

dice fiscale, qualsiasi informazione sulla loro attività e struttura, ecc.

Un'informazione, purché associata o associabile a una persona

Tuttavia non è automatico che un'informazione sia un dato personale. Infatti si definisce "dato personale" solo un'informazione relativa a persona **identificata o identificabile**.

Il contrario del dato personale è il "dato anonimo", vale a dire un'informazione su una persona non identificabile in alcun modo. **Ciò che fa sì che un'informazione sia un "dato personale", in altri termini, è la possibilità di identificare la persona a cui si riferisce.** Se l'informazione è associata a un nome diventa automaticamente un dato personale. Ma lo diventa anche l'informazione non associata a un nome, se si può collegarla a una persona determinata mediante un ragionamento o una tecnica che non richiedano uno sforzo eccezionale. Va sottolineato che **non è necessario che una persona sia effettivamente identificata, basta che possa esserlo almeno in teoria.**

La scheda elettorale da me inserita nell'urna è un tipico dato anonimo, tant'è che viene annullata se ci sono segni che consentirebbero l'individuazione del votante. Invece è quasi sempre un dato personale un'intervista anonima fattami da un operatore che non mi conosce ma che mi chiede alla fine la data di nascita; infatti attraverso di essa e qualche altra informazione si potrebbe risalire a me e quindi identificarmi.

Vediamo se hai capito tutto

La registrazione audio della voce di una persona è un dato personale ? *Si.*

Una ricetta medica è un dato personale ? *Si, se figura il nome della persona o essa è identificabile.*

Una scuola pubblica l'elenco degli alunni portatori di handicap, mettendo al posto del nome le iniziali e la classe frequentata. E' un dato personale? *Si, perché l'interessato è identificabile indirettamente.*

Le impronte digitali prese da apparecchi elettronici per entrare in banca sono un dato personale ? *Si. In questo caso la banca ha l'obbligo di criptarle e di distruggere la registrazione dopo poche ore.*

Le immagini prese da un circuito di videosorveglianza sono dati personali? *Si. In questo caso c'è l'obbligo di informare con un cartello chi entra nel campo di ripresa e di distruggere la registrazione dopo poche ore.*

Lezione 2

L'Interessato è il perno di tutto

Il Codice Privacy definisce "Interessato" la persona fisica, la persona giuridica, l'Ente o l'associazione cui si riferiscono i dati personali.

Ecco chi è il padrone dei propri dati personali. Verso di lui chi raccoglie o detiene i dati ha l'obbligo della **trasparenza assoluta**.

- Un Ente pubblico non deve richiedere il consenso dell'Interessato, ma prima di acquisire o trattare i suoi dati ha l'obbligo di dargli comunque una chiara informativa su modalità e scopi del trattamento.
- Un privato può trattare i dati di un Interessato solamente se questo ha preventivamente acconsentito dopo aver ricevuto apposita informativa su modi e scopi.
- In tutti i casi l'Interessato può in qualsiasi momento verificare quali suoi dati personali sono in possesso di qualsiasi Ente, ditta, etc., e chiederne l'aggiornamento (o anche, in molti casi, la cancellazione).

L'Interessato ha diritto:

che siano rispettate la sua privacy, la sua dignità, la sua identità personale, la sua libertà;

di essere "lasciato in pace, per conto suo", nell'anonimato, di non subire ingerenze, a meno che non sia la legge stessa a imporgli uno specifico obbligo o non sia proprio lui a dare il consenso ad essere oggetto di attenzione altrui;

di essere "dimenticato" quando una pratica è conclusa, distruggendo prontamente i suoi dati, a meno che non sia obbligatorio per legge conservarli.

Chi risponde dei dati personali dell'Interessato? Il TITOLARE

Agli effetti del Codice Privacy si definisce 'Titolare' del trattamento di dati personali la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che utilizza i dati personali di terzi; ad esso competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Tutte le responsabilità sono a carico del cosiddetto 'Titolare' del trattamento dei dati personali.

Nel caso di ditte individuali il Titolare è il proprietario; nel caso di società, enti, associazioni il Titolare è la società stessa o l'Ente stesso. **NON SI DEVE CONFONDERE MAI IL TITOLARE CON IL RAPPRESENTANTE !** Nelle ditte individuali il rappresentante coincide con il Titolare; quando, invece, il Titolare è una società o Ente etc. il rappresentante è il Dirigente che ha il massimo potere decisionale o che è stato a ciò delegato. Negli enti elettivi è l'organo che ha potere decisionale (ad esempio, il Sindaco; però alcuni interpretano diversamente, ripartendo la rappresentanza tra vari organi e dirigenti, in base al potere decisionale di ciascuno, secondo lo Statuto dell'Ente).

Esempio:

Nel caso della scuola pubblica chi è il Titolare ? *Nel caso della scuola è evidente che il Titolare è l'Istituto Scolastico come definito dal Ministero, ovvero l'insieme di unità scolastiche che formano un unico Istituto dotato di autonomia. Ovviamente il Titolare esprime la sua volontà attraverso l'organo che lo rappresenta, cioè il Dirigente Scolastico nel caso della scuola.*

Compiti e poteri del Titolare

Compito del Titolare è applicare il Codice Privacy, **impartendo chiare e rigorose disposizioni scritte ai suoi collaboratori per il trattamento dei dati. Ha anche il compito di controllare che siano applicate. Il Titolare ha la responsabilità amministrativa, civile e penale del rispetto del Codice in materia di protezione dei dati. Non si libera di questa responsabilità nemmeno quando delega** i trattamenti di dati ad altre figure previste dal Codice come esecutori a suo nome dei trattamenti (il "**Responsabile**" e l' "**Incaricato**" di specifici trattamenti). Pertanto, avendo tutte le responsabilità, ha anche tutti i poteri in merito all'applicazione del Codice Privacy.

Chi tratta dati personali deve obbligatoriamente avere una nomina autorizzativa da parte del Titolare (o di un suo delegato, il 'Responsabile').

Il Codice Privacy introduce la novità che **chiunque tratta i dati personali deve previamente ricevere una nomina che lo autorizza a farlo, indicando chiaramente "quali trattamenti" può effettuare, a "quali" banche dati può accedere, con "quali regole e modalità" deve trattare i dati.**

Tale nomina può essere quella di "**Responsabile** del trattamento" o di "**Incaricato** del trattamento". **Il principio basilare è che se un dato personale è trattato da una persona priva della nomina, il trattamento diventa illegittimo e scattano conseguenze gravi.**

Responsabile del trattamento

Il "Titolare" può, a sua discrezione, nominare o meno un "Responsabile del trattamento", a cui delegare una serie di responsabilità che vedremo più oltre. Ha inoltre facoltà di nominare più Responsabili oppure di affidare tale incarico ad un esterno – in questo caso non necessariamente una persona fisica ma anche eventualmente una persona giuridica (per esempio, una società oppure un Ente).

In ogni caso, il Titolare mantiene l'obbligo di dare al Responsabile istruzioni generali **in dettaglio e per iscritto** nonché di eseguire **controlli periodici** e regolari.

Il Responsabile deve effettuare il trattamento attenendosi alle istruzioni impartite dal Titolare. Ha la facoltà di nominare degli Incaricati del trattamento, che dipendono dalle sue direttive e dal suo controllo per quanto riguarda la privacy e protezione dei dati personali.

Incaricati del trattamento

Agli effetti del Codice si definiscono "Incaricati" le persone fisiche autorizzate a compiere operazioni di trattamento di dati personali **mediante apposita nomina** effettuata dal Responsabile (se esiste) o dal Titolare. Possono essere nominati Incaricati solo le per-

sona fisica (anche esterne alla struttura).

Gli Incaricati svolgono una o più delle operazioni che costituiscono “trattamento di dati personali” (vedi la spiegazione dettagliata tra poche righe).

Qualsiasi operazione di trattamento di dati personali (anche la più elementare!) **può essere effettuata solo dal Titolare, dal Responsabile o da Incaricati che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite.**

In pratica, **la nomina a Incaricato equivale ad un’ autorizzazione a fare determinate cose. Nessuno può compiere trattamenti di dati personali se non ne ha l’ autorizzazione, cioè se non è stato nominato Responsabile o Incaricato.** Di conseguenza, per quei dipendenti la cui mansione comporta il trattamento di dati personali, tale autorizzazione è la condizione necessaria ed inderogabile per svolgere il proprio compito: questo spiega perché la nomina a Incaricato non può essere rifiutata.

La designazione a Incaricato è effettuata per iscritto e individua puntualmente l’ ambito del trattamento consentito (= a quali archivi cartacei o informatici può accedere, quali operazioni di trattamento può eseguire), **nonché le regole da seguire. C’ è anche l’ obbligo di dare all’ Incaricato una formazione in materia di Privacy adeguata ai compiti che deve svolgere**, soprattutto se tratta dati sensibili o giudiziari (vedi più oltre la definizione).

Il Codice consente di eseguire anche la **nomina collettiva ad Incaricato**. In pratica per un’ intera unità organizzativa sono individuati, sempre per iscritto, i trattamenti autorizzati per coloro che ne fanno parte e le regole da seguire. Pertanto basta assegnare un dipendente a tale unità organizzativa ed automaticamente diventa Incaricato. Questo vale anche quando un dipendente entra a far parte successivamente dell’ unità organizzativa (ad esempio, un supplente): diventa automaticamente Incaricato (però de- v’ essere informato del fatto, ricevere le istruzioni complete e un’ adeguata formazione).

In particolare, l’ Incaricato deve osservare rigorosamente le misure di sicurezza adottate dal Titolare e dal Responsabile e mantenere l’ assoluto riserbo su tutti i dati personali trattati.

Esistono dipendenti che non trattano mai dati personali (per esempio, un operaio di catena di montaggio, un disegnatore tecnico, ecc.): in questo caso non vengono nominati Incaricati.

Esempio

Un piccolo Comune incarica un fattorino di distribuire il proprio giornale destinato ai cittadini e allo scopo gli dà l’ indirizzario delle famiglie residenti cui attenersi. Deve nominarlo Incaricato? *Si, perché tratta dati personali. Lo ha stabilito il Garante rispondendo a un quesito.*

Attenzione al significato dell’ espressione “trattamento dei dati personali”

L’ espressione “trattamento di dati” è la più usata nel Codice Privacy. Pertanto è fondamentale capire a fondo cosa significa. Al di là dell’ apparente significato del termine, in realtà **per il Codice Privacy significa qualsiasi operazione fatta su dati personali dal momento iniziale della raccolta fino al momento conclusivo della distruzione,**

compreso anche il semplice fatto di detenerli. In particolare, costituisce da sola “trattamento di dati” una qualsiasi delle seguenti azioni, effettuata con o senza l'ausilio di strumenti elettronici:

la raccolta dei dati (in qualsiasi modo effettuata);

il semplice possesso o conservazione dei dati personali;

la gestione dei dati;

la registrazione o l'organizzazione dei dati;

la consultazione (=la visione), il raffronto, l'utilizzo in qualsiasi forma, l'elaborazione o la modificazione dei dati;

la selezione o l'estrazione da un archivio dei dati che interessano

l'interconnessione con altri archivi

il blocco (=congelamento, sospensione temporanea di qualsiasi altro trattamento di certi dati personali: può avvenire su ordine del Garante o decisione del Titolare)

la comunicazione a terzi o la diffusione a chiunque di un dato

la cancellazione o la distruzione di dati, anche se non registrati in una banca dati.

Ribadiamo: **qualsiasi delle operazioni concernenti una di queste “fasi” costituisce “trattamento”.** Il “trattamento” però normalmente è costituito da una serie di queste operazioni.

<p>Perché è importante fare attenzione alla definizione di <u>ciascuna</u> delle attività che da sola costituisce “trattamento” ?</p>
--

Perché ogni trattamento (e quindi ogni sua fase):

può iniziare o continuare solo se è legittimo farlo (cioè deve basarsi su presupposti di legittimità fissati da rigidi principi che vedremo più oltre);

deve essere espressamente autorizzato e controllato dal Titolare;

la persona che lo esegue deve ricevere l'autorizzazione a farlo mediante la designazione scritta a “Incaricato” o “Responsabile” del trattamento stesso;

deve essere effettuato rispettando le modalità regolamentate dal Codice Privacy;

deve essere eseguito per una finalità ben determinata e resa esplicita all'Interessato (spesso è proprio la finalità l'elemento discriminante che rende legittimo o illegittimo il trattamento stesso).

Lezione 3

CLASSIFICAZIONE DEI DATI PERSONALI

Il Codice Privacy classifica i dati personali nelle seguenti categorie: **Dati Identificativi**,

Dati Comuni o Ordinari, Dati Sensibili, Dati Giudiziari.

Questa classificazione tiene conto del **diverso livello di riservatezza delle varie tipologie di dati** e della **diversa pericolosità di un dato per la privacy dell'individuo a cui si riferisce.**

Di conseguenza, **la classificazione di un dato personale in una categoria o in un'altra comporta una fortissima diversificazione delle regole da applicare.**

3.1 Dati identificativi

Sono quei dati personali che permettono l'identificazione diretta dell'interessato: cognome e nome, codice fiscale, partita Iva, codice sanitario, altri codici identificativi. A differenza degli altri dati essi non forniscono alcuna informazione in più sull'Interessato, ma lo identificano.

Dati Comuni (chiamati anche dati ordinari o semplicemente dati personali)

E' impossibile farne un elenco completo, perché i Dati Comuni sono innumerevoli. In pratica sono definibili solo per esclusione: sono quelli che non sono sensibili e non sono giudiziari (vedi definizioni successive). A titolo esemplificativo: dati anagrafici, nome e cognome, indirizzo, residenza anagrafica, indirizzo postale, indirizzo di posta elettronica, numero telefonico, codice fiscale, partita Iva, codice sanitario, qualunque codice identificativo compreso bancomat e carta di credito, etc. e comunque **i dati pubblici in genere.** I dati comuni sono riferibili anche ad enti (sia pubblici che privati), associazioni e società: denominazione sociale, sede, indirizzo, numero di telefono, indirizzo email, codice fiscale, etc. Ma anche valutazioni, profili personali, abitudini, profili professionali, hobbies, gusti gastronomici, preferenze di qualsiasi tipo. E ancora: i numeri di telefono chiamati, il fatto stesso di aver eseguito una telefonata, le telefonate ricevute, il fatto stesso di aver ricevuto una telefonata, lo scontrino del supermercato, ma anche il fatto stesso di aver fatto la spesa al supermercato, e così via...

Dati Sensibili

I Dati Sensibili sono 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**
- **l'adesione a sindacati**

- l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- lo stato di salute (compresi stati quali: handicap, menomazioni fisiche, gravidanza e puerperio, dati genetici e biometrici, infortuni) [la biometria è la misurazione/descrizione di caratteristiche del corpo umano sufficienti a riconoscere un individuo: impronte digitali o dell'iride o della voce, caratteristiche identificatrici del volto, impronte dentali, talune radiografie e simili, ecc.]
- la vita sessuale (=compresi cambio di sesso, omosessualità, inclinazioni particolari).

Cosa significa la locuzione “dati idonei a rivelare”.

Sono sensibili anche quei **dati parziali, apparentemente poco significativi o neutri, che possono essere sufficienti a rivelare indirettamente notizie relative alle sfere personali sensibili**. Per esempio, il fatto che un bambino in mensa chieda una certa dieta (riconducibile alla religione musulmana) è un'informazione idonea a rivelare l'orientamento religioso e quindi va classificata come dato sensibile. Lo stesso vale per una dieta rivelatrice di una patologia. E così via.

In genere un certificato medico (anche privo di diagnosi!) per l'assenza dal lavoro o da scuola è considerato un dato idoneo a rivelare lo stato di salute; perfino il registro delle assenze e altre registrazioni di questo tipo sono considerati idonei a rivelare lo stato di salute, pertanto vanno trattati con le cautele previste per i dati sensibili.

Finora il Garante della Privacy ha sempre dato l'interpretazione più estesa del concetto di “dato idoneo a rivelare”.

E' importante sottolineare che tutto ciò che si riferisce a persona con handicap, se individuabile, è dato sensibile.

Dati Giudiziari

I Dati Giudiziari sono quei Dati Personali idonei a rivelare:

l'iscrizione nel casellario giudiziale a seguito di condanna penale (compresa l'iscrizione nell'anagrafe delle sanzioni amministrative dipendenti da reato);

la qualità di imputato o di indagato.

Fanno parte di questa categoria anche quei dati che sono idonei a rivelare, pur indirettamente, una di queste situazioni.

Perché è importante riconoscere i Dati Sensibili e Giudiziari

Dal fatto che un dato sia da noi classificato come sensibile o giudiziario, discendono conseguenze pratiche e giuridiche discriminanti. Se un dato personale è “sensibile” o “giudiziario”, **scattano per il Titolare e per tutto il personale regole particolari**, molto impegnative, riguardo a:

le condizioni che rendono legittimo il trattamento oppure certe operazioni (es. la comunicazione o la diffusione). Per autorizzare la raccolta stessa del dato e il suo trattamento ci può volere una legge o un regolamento legislativo o un'autorizzazione del Garante per la protezione dei dati personali);

il tipo di informativa da dare all'Interessato;

la custodia con misure di sicurezza adeguate alla delicatezza dell'informazione da proteggere (per esempio i dati relativi alla salute registrati in un computer devono essere cifrati).

La violazione di queste regole inibisce automaticamente l'uso dei dati e comporta sanzioni estremamente pesanti.

Un errore di classificazione può, quindi, comportare violazioni conseguenti, punite con sanzioni amministrative o penali severissime e con risarcimento dei danni materiali e morali subiti dall'Interessato, in quanto la norma (art. 15) è costruita in modo da rendere più facile la vittoria dell'Interessato che, sentendosi danneggiato, promuove causa civile.

Dati particolari o quasi-sensibili

E' un'ulteriore categoria intermedia tra Dati Sensibili e Comuni, il cui trattamento presenta rischi specifici per i diritti e le libertà fondamentali ovvero per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare. Fa parte della filosofia del D.Lgs 196/2003 l'obbligo per chi tratta i dati personali di valutare se essi, benché non rientrino nelle categorie definite sensibili, siano in grado comunque di minacciare i beni personali protetti (dignità, diritti, libertà); in tal caso scatta una responsabilità a trattare con adeguata cautela anche tali dati.

Il trattamento dei dati particolari è soggetto ad accorgimenti a tutela dell'Interessato. La sanzione per la violazione di questa regola va da € 5.000 a € 30.000 (il minimo effettivamente sanzionato è però € 10.000).

A titolo di esempio, rientrano sicuramente in questa categoria casi del tipo:

lo stato di adozione o di affidamento di un minore;

l'informazione che una signora è una prostituta (non è un dato giudiziario, ma lede la dignità);

particolari immagini foto o video che potrebbero ledere la dignità;

provvedimenti disciplinari o note che non si ha diritto di divulgare (potrebbero ledere il diritto al lavoro o altri diritti o la dignità della persona),

Sia chiaro che **questi dati possono essere trattati per finalità** lecite e se il trattamento è pertinente, necessario e non eccedente rispetto alla finalità; **la violazione consiste nel trattarli fuori di questi casi oppure nella conservazione senza le dovute cautele o nella comunicazione o diffusione non necessaria.**

Cos'è la "comunicazione di dati"

La comunicazione di dati personali è una dei trattamenti più delicati. **Questa operazione è spesso vietata o soggetta a restrizioni e a particolari condizioni; la violazione di queste regole è sanzionata in modo pesantissimo.** Pertanto è fondamentale la definizione di "comunicazione" e ogni operatore deve saperla riconoscere e distinguere con assoluta sicurezza.

Il Codice definisce "comunicazione": il **dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'Interessato**, in qualunque forma, anche mediante la loro messa a disposizione o **consultazione**. "Soggetti determinati" significa

identificati o identificabili in modo univoco e preciso. In sostanza, si parla di comunicazione quando il Titolare sa a priori "chi" esattamente vedrà o riceverà i dati.

La lettera in busta chiusa è il caso più tipico di comunicazione. Ma lo è anche un'informazione data per telefono, un fax o un messaggio di posta elettronica. Così pure una foto, una radiografia, un documento, una registrazione video mostrati o consegnati a qualcuno. E ancora: una registrazione audio fatta ascoltare o consegnata. Il punto è se la conoscenza è limitata a soggetti determinati, come sopra spiegato.

Esempio

La lettera alla Questura in cui si comunica l'infortunio di un dipendente è una comunicazione? *Sì, perché la Questura è un soggetto determinato (non importa quale funzionario specificamente leggerà la lettera).*

Dare temporaneamente un documento da consultare a una persona è una comunicazione?

Sì, se tale persona è identificata.

In una riunione con i genitori degli alunni, conosciuti come tali, dare informazioni sulle Ditte in cui realizzare stages è una comunicazione? *Sì, perché si tratta di soggetti determinati.*

Non si considera comunicazione lo scambio di dati interno all'Ente (o con soggetti incaricati formalmente di svolgere attività per conto dell'Ente stesso). Ovviamente sono consentite senza limiti le comunicazioni di dati fra Incaricato e Responsabile (anche esterno) o Titolare; anzi in senso stretto non sono nemmeno considerate comunicazioni ai sensi del Codice Privacy.

La comunicazione di dati è soggetta a gravi limitazioni e sanzionata in caso di abuso, pertanto è opportuno chiedersi sempre se chi riceve l'informazione ne ha diritto. In caso di dubbio, va chiesta l'autorizzazione al superiore. In particolare devono essere osservate rigorosamente le misure di sicurezza adottate dal Titolare e dal Responsabile e mantenere l'assoluto riserbo su tutti i dati personali trattati.

Perché il Codice prevede queste forti limitazioni alla comunicazione ?

I motivi per le forti limitazioni alla comunicazione sono essenzialmente di due tipi. Se il Cittadino affida i propri dati a uno specifico Ente, quando essi sono comunicati ad altri, in parte egli perde il controllo dei flussi di dati che lo riguardano e delle garanzie con cui vengono trattati, quindi è necessario che:

egli sia puntualmente informato di ciò al momento in cui consegna i dati (l'informativa deve indicare che ci sarà una comunicazione di dati e a chi o a quale tipo di destinatario !)

la comunicazione avvenga soltanto se realmente necessaria e comunque solo in presenza di norme di legge o di autorizzazioni del Garante che la consentano o la prevedano (un Ente Pubblico, come si vedrà più oltre, potrà anche dotarsi di un regolamento che autorizzerà certe comunicazioni)

la comunicazione si limiti agli elementi strettamente pertinenti e indispensabili alla finalità da raggiungere.

Inoltre, il Codice Privacy vuole impedire che più Titolari mettano in comunicazione fra loro i rispettivi archivi creando così di fatto un super-archivio con una tale concentrazione di dati personali che diventerebbe una minaccia per il diritto alla riservatezza del cit-

tadino e anche per la sua libertà.

Cos'è la "diffusione di dati"

Il Codice definisce "diffusione": il **dare conoscenza dei dati personali a soggetti indeterminati**, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. In pratica il Titolare non sa a priori "chi" vedrà o riceverà i dati: ad esempio, se espongono all'albo un documento, non posso prevedere esattamente né quante né quali persone lo vedranno. In pratica **un dato diffuso è potenzialmente reso noto a tutti**. Tipici esempi di diffusione sono la pubblicazione su manifesti, su giornali, l'esposizione all'albo ovvero la pubblicazione nel sito internet dell'Ente o mettere il fascicolo con le graduatorie su un banco nell'atrio per cui possa essere consultato da chiunque.

Va sottolineato che la diffusione dei dati, quando non è espressamente consentita dalle norme, è una delle infrazioni più gravi, perché l'Interessato viene come spodestato definitivamente di quei dati personali e viene definitivamente privato della riservatezza. Perciò la diffusione di dati è dinamite: è punita con gravi sanzioni, ma soprattutto è automatica la condanna da parte di un tribunale civile a rifondere i danni materiali e morali.

Perciò qualsiasi operatore deve chiedere preventivamente espressa autorizzazione al superiore prima di operare una diffusione.

In particolare **è sempre vietato diffondere dai relativi allo stato di salute** (a meno che non sia l'Interessato a delegare un Titolare a farlo, come nel caso di calciatori professionisti che delegano espressamente la loro Società a farlo).

Le eccezioni

Ci sono però **atti che per definizione sono pubblici** e possono essere diffusi. Esempio: elenchi telefonici recanti i dati di chi accetta di essere inserito, in quanto vuole che chiunque lo cerchi possa trovare il modo di telefonargli. Idem per i nominativi degli iscritti ad albi professionali (in tal caso serve anche per consentire a chiunque di verificare che il professionista a cui intende rivolgersi possenga realmente una certa qualifica).

Ci sono anche **atti che è obbligatorio per legge rendere pubblici**, affinché ci sia un controllo sociale: graduatorie di posti pubblici, risultati di concorsi, ditte partecipanti a gare d'appalto, redditi dei pubblici amministratori, tabelloni degli esiti scolastici, ecc.

I motivi per le forti limitazioni alla diffusione

Se il Cittadino affida i propri dati a uno specifico Ente, quando essi sono diffusi (= resi noti potenzialmente a chiunque), la minaccia al suo diritto alla riservatezza è massima, quindi è necessario che:

egli sia puntualmente informato di ciò al momento in cui consegna i dati (l'informativa deve indicare che ci sarà una diffusione di dati!)

la diffusione avvenga soltanto se realmente necessaria e comunque solo in presenza di norme di legge o regolamento legislativo o di autorizzazioni del Garante
la diffusione si limiti agli elementi strettamente pertinenti e indispensabili alla finalità da raggiungere.

Lezione 4

REGOLE PER IL TRATTAMENTO DI DATI PERSONALI

Rispetto ai privati e agli enti pubblici economici (che quindi non perseguono un interesse pubblico puro, bensì si muovono nell'ambito del mercato), **per i soggetti pubblici il Codice prevede regole speciali relativamente all'informativa e per il diritto di trattare i dati, di comunicarli e di diffonderli.**

Inutilizzabilità dei dati trattati in violazione delle regole del Codice Privacy

"I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati." Questo principio (art. 11) è inderogabile e la sua violazione, negli enti pubblici, potrebbe comportare la nullità degli atti, con tutte le gravi conseguenze del caso! Pertanto, le regole illustrate di seguito e nei prossimi capitoli devono essere ben studiate e applicate.

Obbligo di informativa completa PRIMA di qualunque trattamento

E' una delle regole fondamentali. Il modo in cui viene data l'Informativa condiziona i trattamenti successivi.

L'Interessato deve essere previamente informato **oralmente o per iscritto** circa

- 1) le finalità del trattamento cui sono destinati i dati (da notare che i dati non potranno poi essere utilizzati per scopi diversi, altrimenti bisogna dare un'integrazione di informativa !);
- 2) le modalità del trattamento (cartaceo, elettronico, raccolta fotografica, raccolta audio, ecc.);
- 3) la natura obbligatoria o facoltativa del conferimento dei dati personali;
- 4) le conseguenze di un eventuale rifiuto di rispondere;
- 5) 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;
- 6) i diritti di cui gode l'Interessato (diritto di accesso ai dati, di loro verifica ed eventuale richiesta di integrazione o eliminazione, ecc.);
- 7) gli estremi identificativi del Titolare e di almeno un Responsabile, se esiste.
- 8) Nel caso di dati sensibili o giudiziari, gli enti pubblici hanno l'obbligo di effettuare un'aggiunta speciale all'informativa, comunicando in base a quale norma i dati vengono trattati (ad esempio, per una prativa relativa a benefici dipendenti dallo stato di gravidanza, va indicata la legge sulla maternità; e così via per ogni dato sensibile).

Si tratta di un elenco tassativo! Devono essere adeguatamente illustrati tutti i 7 elementi sopra elencati, più l'ottavo se si è in presenza di dati sensibili o giudiziari.

sa comporta la mancanza dell'informativa (anche di uno soltanto dei suoi componenti tassativi) ?

La mancanza dell'informativa o l'inadeguatezza della stessa potrebbe causare l'**illegittimità degli atti conseguenti**, fino a causarne la **possibile nullità**. Inoltre, è punita con una **sanzione amministrativa che va da € 3.000 a € 18.000** (con un minimo effettivo di € 6.000!).

Se c'è mancanza o inadeguatezza del punto 8 oppure si tratta di Dati che, pur non essendo Sensibili o Giudiziari, presentano però rischi specifici per le libertà fondamentali o la dignità dell'individuo, la sanzione è maggiore.

Sul fatto di non dimenticare mai di dare l'informativa è necessario il massimo impegno di qualunque dipendente che riceva o comunque acquisisca un dato personale nuovo.

Quando va data l'Informativa ?

Dev'essere data prima di cominciare il trattamento dei dati. Solo nel caso di dati ricevuti da terzi, va data all'interessato prima della loro registrazione o, se è prevista la comunicazione dei dati, va data contemporaneamente o prima della prima comunicazione all'Interessato.

Serve il consenso dell'interessato? Serve la sua firma?

Il D.Lgs 196 all'art. 18 esclude esplicitamente che gli enti pubblici chiedano il consenso dell'Interessato. Pertanto non serve né il consenso scritto né quello orale, basta dare l'informativa.

Poiché sono previste gravi sanzioni per la non effettuazione dell'informativa o per la sua effettuazione incompleta, è consigliabile **conservare comunque una prova di averla data.** Intanto è **opportuno dare un'informativa scritta**, perché resta agli atti ed è sempre documentabile. Poi **serve una prova che l'Informativa sia stata data all'Interessato:** una firma di semplice ricevuta da parte dell'Interessato o un'annotazione del dipendente che ha dato l'informativa.

Nel caso di minorenni, l'informativa va data a chi esercita la patria potestà.

Se i dati personali da trattare riguardano anche un familiare o un terzo, anch'essi hanno diritto all'informativa e l'Ente ha il dovere di dargliela prima di cominciare il trattamento dei dati (sottolineiamo che l'informativa dev'essere data prima dell'inizio di tale trattamento).

N.B.: Considerata l'importanza dell'Informativa e i rischi connessi, gli addetti che in qualunque modo sono deputati all'acquisizione di dati dovrebbero approfondire l'argomento con la specifica dispensa (la quale reca, tra l'altro, esemplificazioni dettagliate sul punto 8, che è quello più difficile).

Regole generali per il trattamento di dati personali

I dati personali devono essere:

trattati in modo lecito e secondo correttezza.

esatti ed aggiornati (pertanto chi li detiene deve farsi ragionevolmente carico del controllo e dell'aggiornamento).

raccolti e registrati solo per finalità legittime, determinate ed esplicite (cioè è vietato raccogliere dati per scopi generici; va chiaramente indicata nell'informativa una finalità specifica ed essa deve essere esplicita, cioè chiaramente espressa all'Interessato).

utilizzati in altre operazioni di trattamento soltanto in termini compatibili con tali finalità.

pertinenti rispetto alle finalità per le quali sono raccolti o successivamente trattati. In pratica, bisogna chiedersi per ogni dato: è davvero pertinente allo scopo di questa operazione?

non eccedenti rispetto alle finalità (la raccolta dei dati vece essere rigorosamente limitata a quelli strettamente necessari per la finalità dichiarata !). In pratica, bisogna chiedersi per ogni dato: è davvero necessario per lo scopo di questa operazione?

Proporzionali allo scopo: ci vuole senso di misura sulla quantità e qualità dei dati che si utilizzano rispetto allo scopo da raggiungere da raggiungere in ciascuna operazione di trattamento

conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati (se la legge prevede che i dati per una certa pratica siano conservati per un determinato numero di anni, la pratica s'intende conclusa e raggiunto lo scopo solamente decorso tale termine).

Successivamente al raggiungimento delle finalità dichiarate, i dati devono essere distrutti (oppure conservati solo in una forma che non consenta l'identificazione dell'Interessato; ad esempio cancellando il nome ecc.). L'obbligo qui previsto trae origine dal fatto che il Codice Privacy vuole impedire che siano accumulati nel tempo troppi dati, creando un super-archivio potenzialmente pericoloso. Inoltre, il diritto alla riservatezza implica che, una volta cessato il trattamento, l'Interessato riprenda il più presto possibile il pieno controllo dei suoi dati personali e della sua privacy.

I dati personali trattati in violazione di queste e altre regole rilevanti non possono essere utilizzati e, nelle pubbliche amministrazioni, il procedimento amministrativo rischia di divenire nullo. L'Interessato può ottenere il blocco del trattamento chiedendolo al Garante a o alla Magistratura.

Un esempio di applicazione dell'obbligo che i dati siano esatti e aggiornati

Il Garante ha accolto il ricorso di un laureato insoddisfatto dell'operato dell'Ente al quale aveva chiesto invano l'aggiornamento dei dati relativi al titolo di studio appena conseguito e l'attestazione che la variazione fosse stata portata a conoscenza di tutti coloro ai quali i dati erano stati comunicati. Il Garante ha stabilito che le aziende private e le pubbliche amministrazioni devono aggiornare i propri archivi con le qualifiche professionali ed i titoli di studio acquisiti dai lavoratori. Tale operazione deve essere tempestiva ed effettuata in ogni altro pertinente data base dell'azienda.

Inutilizzabilità dei dati trattati in violazione delle regole del Codice Privacy

Ripetiamo : “I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.” Questo principio (art. 11) è inderogabile e la sua violazione, negli enti pubblici, potrebbe comportare la **nullità degli atti**, con tutte le gravi conseguenze del caso ! Pertanto, le regole illustrate di seguito e nei prossimi capitoli devono essere ben studiate e applicate.

Quando un Ente Pubblico è autorizzato a trattare Dati Comuni Non Sensibili e Non Giudiziari (con l'esclusione di comunicazioni e diffusionsi che hanno diversa regolamentazione)

I soggetti pubblici hanno l'autorizzazione al trattamento di tutti quei Dati che non siano Sensibili né Giudiziari, purché siano necessari all'attività istituzionale. Non serve una norma di legge o un regolamento legislativo che autorizzi il trattamento di tali dati.

Principio di finalità istituzionale: sono consentiti soltanto trattamenti di dati personali per lo svolgimento delle funzioni istituzionali.

E' una norma tassativa, che non lascia margini di discrezionalità ad alcuna pubblica amministrazione per decidere quali dati raccogliere e quali trattamenti eseguire.

Per funzione istituzionale s'intende ovviamente l'insieme delle finalità per cui l'ente è stato istituito, così come fissate dalla legge e da eventuali regolamenti generali applicabili al settore. Tuttavia sono riconducibili alla finalità istituzionale anche i trattamenti che sono strumentali per la realizzazione degli interessi pubblici affidati a tale ente (esempio: eseguire i trattamenti relativi all'acquisto della carta su cui scrivere i documenti non è certo la funzione diretta di un ente, tuttavia è uno scopo strumentale alle funzioni istituzionali). Ma attenzione! Non si può con questo ragionamento ricondurre indirettamente qualsiasi cosa all'attività istituzionale.

I dati acquisiti o comunque trattati trasgredendo il **Principio di necessità** o il **Principio di finalità istituzionale** rendono illegittimo o nullo l'atto amministrativo e non possono comunque essere utilizzati; inoltre, costituiscono infrazione al Codice.

Questi principi sono posti per impedire che l'ente pubblico si giovi delle regole più favorevoli a cui è sottoposto – non occorre il consenso dell'Interessato per trattare i dati! – e della propria posizione egemone rispetto all'utente (= possibilità di ritardare il servizio se l'Interessato non comunica qualsiasi dato richiesto), per procurarsi indebitamente dei dati personali.

Un esempio di pronuncia del Garante sul Principio di finalità istituzionale

Un Comune ha chiesto al Garante se poteva installare delle telecamere in luoghi pubblici per la raccolta di prove di eventuali atti di vandalismo, danneggiamenti o altri atti criminosi, affinché si potessero perseguire penalmente e civilmente i relativi autori. Si noti che le riprese di telecamere sono dati personali. Il Garante ha risposto che era un trattamento illecito perché il Comune era privo di funzioni istituzionali in materia di prevenzione ed accertamento dei reati; solo le forze di Polizia erano legittimate a farlo.

Quando un Ente Pubblico è autorizzato a comunicare Dati Comuni ad altri enti pubblici

Quando tale comunicazione è necessaria per lo svolgimento delle funzioni istituzionali ed è prevista da norma di legge o regolamento legislativo, entro i limiti da questi stabiliti; se manca la legge, si può chiedere l'autorizzazione al garante.

In assenza di una norma di legge o di regolamento legislativo questo tipo di comunicazione è proibita. Il realizzarsi delle condizioni sopra elencate è un tassativo presupposto di legittimità della comunicazione. Significa che al di fuori di questi criteri, la comunicazione diviene illegittima, può comportare nullità degli atti e, in certi casi, reato penale punito con l'arresto.

Quando un Ente Pubblico è autorizzato a comunicare Dati Comuni a privati

Simile al precedente.

DEROGHE

Dati degli studenti a fini di orientamento, *stages* o inserimento professionale (ma su loro richiesta); finalità di difesa dello Stato, di sicurezza pubblica, prevenzione o repressione di reati.

Esempi di pronuncia del Garante

Un partito politico ha chiesto al comune l'elenco dei capifamiglia. Il comune lo ha negato. Il garante ha stabilito che era vietato, perché non è previsto da alcuna legge, quindi questa comunicazione è vietata.

Quando un Ente Pubblico è autorizzato a diffondere Dati Comuni

Quando tale diffusione è **necessaria** per lo svolgimento delle funzioni istituzionali ed è **esplicitamente prevista da norma di legge o regolamento legislativo**, entro i limiti da questi stabiliti; inoltre **l'Informativa deve averlo indicato**.

Il realizzarsi delle condizioni sopra elencate è un tassativo presupposto di legittimità della diffusione. Significa che al di fuori di questi criteri, la diffusione diviene illegittima, può comportare nullità degli atti e, in certi casi, reato penale punito con l'arresto.

In assenza di una norma di legge o di regolamento generale che esplicitamente preveda la diffusione, essa è proibita.

La pubblicazione di dati sul sito web dell'Ente equivale a diffusione. Pertanto va valutato con grande attenzione quali nomi, foto riconoscibili e dati si è realmente autorizzati a pubblicare !

Naturalmente, l'Ente Pubblico ha spesso addirittura l'obbligo di legge di diffondere dati, nel caso di graduatorie di concorsi, esiti di esami e scrutini, appalti di opere pubbliche, ecc. In questi casi **lo spirito della legge è che determinate informazioni devono essere conoscibili da tutti affinché l'opinione pubblica eserciti un controllo sull'operato dell'ente.**

Esempi di pronuncia del Garante

Il garante ha stabilito che la divulgazione dei redditi dei giudici tributari era legittima in quanto prevista dalla legge sulla trasparenza amministrativa (Legge 127/1997 Bassani-bis).

Il garante ha stabilito che l'ufficio di collocamento non può comunicare a un datore di lavoro privato la lista degli iscritti al collocamento perché la legge prevede che sia comunicabile solo a determinati soggetti privati (quelli autorizzati alla mediazione).

Quando un Ente Pubblico è autorizzato a trattare e comunicare Dati Sensibili o Giudiziari (esclusa la diffusione che ha una diversa regolamentazione)

Nel caso di dati sensibili e giudiziari, che sono più delicati, viene introdotto il **Principio di indispensabilità**.

Il Principio di indispensabilità è più restrittivo del principio di necessità : quindi questi dati possono essere trattati, comunicati e diffusi solo quando non se ne può proprio fare a meno.

Il trattamento e la comunicazione (ma non la diffusione) dei dati sensibili da parte di un Ente pubblico sono consentiti solo se si realizzano **tutte insieme queste 4 condizioni**:

- a) tali dati servono per **finalità istituzionali** e sono **strettamente indispensabili**;
- b) l'uso di tali dati è **autorizzato da espressa disposizione di legge**;
- c) **tale legge specifica i tipi di dati trattabili e le operazioni eseguibili** (questo punto può essere sostituito da un Regolamento dell'Ente);
- d) **tale legge indica le finalità di rilevante interesse pubblico perseguite** (questo punto può essere sostituito da un' Autorizzazione del garante).

Il realizzarsi congiunto delle 4 condizioni sopra elencate è un tassativo presupposto di legittimità del trattamento. Significa che al di fuori di questi criteri, il trattamento diviene illegittimo, può comportare nullità degli atti e, in certi casi, reato penale punito con l'arresto.

Quando un Ente Pubblico è autorizzato a diffondere Dati Sensibili o Dati Giudiziari

Sono indispensabili due condizioni congiunte: tale diffusione deve essere INDISPENSABILE per lo svolgimento delle funzioni istituzionali e deve essere esplicitamente prevista da norma di legge.

Il realizzarsi delle condizioni sopra elencate è un tassativo presupposto di legittimità della diffusione. Significa che al di fuori di questi criteri, la diffusione diviene illegittima, può comportare nullità degli atti, risarcimento dei danni morali e materiali, e, in certi casi, reato penale punito con l'arresto.

E' sempre vietato diffondere dati sensibili idonei a rivelare lo stato di salute

Un esempio

Un'insegnante elementare ha segnalato al Garante di non aver avuto idoneo riscontro ad una richiesta rivolta al competente provveditorato agli studi, con la quale chiedeva la cancellazione o la trasformazione in forma anonima della dicitura "portatore di handicap" che compariva accanto al proprio nome, in un elenco di lavoratori trasferiti presso altre sedi. La questione aveva determinato per l'insegnante una situazione di grave disagio a livello personale e di relazione con gli altri colleghi.

L'Autorità, accogliendo il ricorso, ha precisato che la divulgazione (=diffusione) del dato sanitario dell'insegnante era illecita perché avvenuta in violazione della legge che vieta la diffusione di dati idonei a rivelare lo stato di salute delle persone. E' stato perciò vietato al Ministero di diffondere ulteriormente, anche presso altri uffici, accanto al nome dell'insegnante, la formula "portatore di handicap", imponendo all'amministrazione la sostituzione con diciture generiche o codici numerici. Non è stata, invece, ritenuta idonea la soluzione di sostituire la dicitura con l'apposizione del riferimento normativo (legge 104/92). Ciò perché il riferimento ad una legge che tutela specificamente le persone disabili finirebbe, anche se in via mediata, per rivelare comunque informazioni sulle condizioni di salute degli interessati.

Enti pubblici: Modalità da applicare al trattamento di Dati Sensibili e Giudiziari

Il principio di fondo della legge è che **devono essere usate modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'Interessato.**

Le regole basilari sono le seguenti.

- Possono essere trattati solo i **Dati Sensibili e Giudiziari indispensabili**.
- Vanno raccolti direttamente dall'interessato, salvo impossibilità inopportunità.
- Nel caso in cui Dati Sensibili o Giudiziari vengano **gestiti mediante computer**, vanno trattati con **tecniche di cifratura** o **sostituendo il nome dell'Interessato con un Codice identificativo** in modo da renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di **identificare gli interessati solo in caso di necessità**. Serve un apposito programma per farlo.

Nel caso di dati idonei a rivelare **lo stato di salute** e la vita sessuale è indispensabile : **conservare separatamente dagli altri dati personali trattati per finalità che non richiedono l'utilizzo dei predetti dati (probabilmente è opportuno chiuderli in busta chiusa, eventualmente riponendola in altro luogo e sostituendo il documento con un foglio generico che ne indichi l'ubicazione);**

se gestiti mediante elenchi, registri o banche dati cartacee, ricorrere a soluzioni che li rendano temporaneamente non comprensibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità. La norma si riferisce a quelle pur rare circostanze in cui si devono eseguire analisi o statistiche del ricorrere di certi casi a prescindere dall'identificazione dell'interessato (ad esempio: numero di portatori di handicap, numero di assenze per malattia o per gravidanza, ecc.): bisogna farlo consultando i dati relativi alla salute o alle abitudini sessuali senza poter vedere il nome dell'Interessato. La norma obbliga a predisporre già da subito la archivi a questo tipo di consultazione e

non attendere che si verifichi la circostanza dell'operazione indicata. Il caso più frequente riguarda il Registro delle assenze, le schede assenze e simili. In alcuni casi la soluzione è un registro con la pagina dei nomi pieghevole, che può restare nascosta consentendo una consultazione anonima. Per le schede, ecc. è più difficile trovare una soluzione, pertanto è meglio ricorrere a schede informatiche.

In conclusione

Il Titolare e/o il Responsabile rende note agli Incaricati regole operative ben precise nel trattamento dei dati, indicando quali tipi di dati può trattare e quali operazioni può svolgere, a quali archivi può accedere e con quali regole. Il Titolare dà istruzioni affinché la comunicazione o diffusione di dati avvengano solo nei casi consentiti. Nei casi dubbi, il dipendente deve chiedere l'autorizzazione al Titolare o al Responsabile, in quanto soltanto essi possono prendersi la responsabilità di valutare se è un caso consentito.

Attenzione ! Per esempio, se un dipendente consegna a una scuola privata l'elenco generale degli iscritti commette un reato penale.

Ogni dipendente deve sempre chiedersi se ogni dato che tratta è pertinente, non eccedente, proporzionato, necessario (INDISPENSABILE se dato sensibile o giudiziario) rispetto all'operazione da fare e alla finalità.

Lezione 6

Principio generale enunciato dal Codice Privacy : “Chiunque ha diritto che i dati personali che lo riguardano siano protetti”.

REGOLE PER LA SICUREZZA

E' obbligatorio applicare queste regole generali.

- Il trattamento dei dati personali deve svolgersi assicurando un **elevato livello di tutela dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato**. Sono parimenti protette la riservatezza e l'identità personale (= la personalità, la storia di un cittadino, la sua figura come appare socialmente e come espressione della sua cultura).
- **Qualunque sistema informatico dev'essere impostato in modo da utilizzare il minor numero di dati personali e, dove è possibile, codici che permettano di identificare l'interessato solo in caso di necessità.**
- **Tutti i dati personali oggetto di trattamento devono essere custoditi e controllati in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta o di perdita dei dati.**

Infine l'**art. 31** obbliga ad aggiornare continuamente le misure di sicurezza “in relazione alle conoscenze acquisite in base al progresso tecnico”.

Le Misure di sicurezza

Le regole generali si traducono in una serie di **specifiche misure di sicurezza**, dette “**misure minime**” di sicurezza perché è il **minimo che è comunque obbligatorio realizzare** (la non attuazione di una o più delle misure minime di sicurezza comporta reato penale punito con ammenda da € 10.000 a € 50.000 o con la reclusione fino a 2 anni).

Le **misure di sicurezza** consistono nel complesso delle **misure organizzative, tecniche, logistiche, informatiche, logiche e procedurali** volte a **ridurre al minimo i rischi** :

di conoscenza da parte di terzi che non hanno l'autorizzazione;

di accesso non autorizzato ai dati;

di trattamento non consentito o non conforme alle e finalità della raccolta;

di alterazione dei dati in conseguenza di interventi non autorizzati o non conformi alla regole;

di distruzione o perdita, anche accidentale, dei dati.

Le misure di sicurezza devono essere differenziate e graduate tenendo conto:

della natura dei dati (più sono “sensibili” o “appetibili” da terzi maggiore deve essere la sicurezza con cui sono protetti);

dei rischi insiti nello specifico trattamento (si deve anche considerare le specifiche caratteristiche del trattamento, in modo che le misure di sicurezza coprano tutti gli aspetti e le modalità).

Un esempio: un caso di furto del computer

È stato compiuto un accertamento ispettivo nei confronti di un policlinico universitario, dove erano stati segnalati alcuni furti di computer. In questo caso, è stato tuttavia accertato *in loco* il rispetto della normativa sulla protezione dei dati personali e, in particolare, l'adozione delle "misure minime" di sicurezza (ispezione presso l'Azienda ospedaliera universitaria Policlinico Federico II). Commento: chi aveva rubato i computers poteva leggere dati sensibili ivi memorizzati. Pare che Garante abbia chiesto a Polizia o Carabinieri di verificare questa possibilità nel caso che qualcuno denunci il furto di computers.

Il Documento Programmatico Sulla Sicurezza (DPS)

E' la principale delle cosiddette "misure minime" di sicurezza; però **redigere il "documento programmatico sulla sicurezza" è obbligatorio soltanto per chi tratta Dati Personali Sensibili o Giudiziari con strumenti elettronici**. In realtà, per chi gestisce i dipendenti col computer o fa uso sistematico delle risorse informatiche è quasi impossibile non trattare dati sensibili o giudiziari, pertanto ha l'obbligo di redigere il DPS.

E' un documento annuale, da adottare entro il 31 marzo di ogni anno [chi lo fa per la prima volta ha il termine ora slittato al 31.12.2005]. Il Titolare di un trattamento di dati sensibili o di dati giudiziari redige (anche attraverso il Responsabile, se designato) un documento programmatico sulla sicurezza contenente in estrema sintesi :

il censimento di tutti i trattamenti di dati;

il censimento di tutti gli archivi cartacei ed elettronici, indicando quali contengono dati sensibili e giudiziari;

il progetto di come saranno attuate tutte le misure minime obbligatorie;

la valutazione accuratissima di tutti i rischi che potenzialmente incombono sui dati (dall'incendio all'errore umano che cancella un disco, dal furto al guasto, ecc.), dando un giudizio sulla loro gravità e sulla probabilità che gli eventi temuti si verifichino realmente (questo punto sarà ampiamente sviluppato tra breve);

un progetto conseguente alla valutazione dei rischi, che descriva gli interventi da fare immediatamente o in fasi successive per adeguare lo stato della sicurezza dei dati stessi, nonché la protezione delle aree e dei locali interessati;

l'analisi della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (il cosiddetto "mansionario privacy");

un programma di adeguati interventi formativi degli Incaricati del trattamento conseguente alle valutazioni precedenti e al ruolo di ciascuno;

la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del Titolare.

ANALISI DEI RISCHI CUI SONO SOGGETTI I DATI

Questo punto potrà sembrare sviluppato in modo troppo dettagliato, però è il Codice privacy che indica questo argomento come il principale da sviluppare. Uno specifico Incaricato potrebbe dire che certi rischi non riguardano la sua attività concreta e quindi è inutile conoscerli. Però altri colleghi in azienda devono affrontarli mettendo in campo adeguate contromisure di sicurezza, perciò è indispensabile che gli altri dipendenti comprendano il perché di certe regole o di certe organizzazioni del lavoro o della presenza di certi strumenti. Comunque, ogni Incaricato è interessato direttamente da almeno qualcuno dei rischi qui analizzati. Deve far riflettere questo esempio: <<Luigi è l'usciera del Comune ed è abituato a andare ogni giorno nell'ufficio del suo amico Antonio, impiegato, a salutarlo. Un giorno Antonio gli dice che non può più entrare nel suo ufficio a causa della 196. Luigi non capisce e pensa che Antonio sotto sotto sia arrabbiato con lui, anche se non ne comprende il perché. Il giorno seguente Antonio gli spiega che si tratta di ordini del suo capo, così Luigi pensa che si tratti di una discriminazione fatta per cattiveria o per eccesso di zelo. Allora Antonio gli dà da leggere questo manuale e finalmente Luigi se ne fa una ragione. >>.

Ogni Titolare ha l'obbligo di analizzare a fondo i rischi a cui sono esposti i dati personali da lui gestiti.

L'analisi dei possibili rischi va effettuata combinando due tipi di valutazioni.

L'appetibilità per gli estranei dei dati trattati, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono: è evidente che dati poco appetibili sono meno esposti al rischio di sottrazione; è altrettanto chiaro che dati sensibili e comunque delicati vanno protetti maggiormente perché il danno possibile per l'Interessato è grave.

Le caratteristiche degli strumenti utilizzati, degli ambienti e delle procedure seguite.

I rischi possono essere dovuti a eventi casuali oppure originati da dolo, da comportamenti degli operatori o da comportamenti illeciti di estranei.

A - Rischio legato a comportamenti umani

- **Impreparazione o distrazione** : informativa data in modo incompleto riguardo uno dei fattori obbligatori (tutte le finalità dei trattamenti, tutte le categorie a cui i dati vengono comunicati o se vengono diffusi, ecc.); dimenticanza di dare l'informativa a tutti i soggetti aventi diritto (in particolare i familiari) o di rinnovarla in caso di trattamenti nuovi o di compimento della maggiore età dell'Interessato; dimenticanza di chiedere il consenso al trattamento, quando dovuto; inizio del trattamento di dati senza l'informativa / consenso o prima di averli; non riconoscimento di dati sensibili o giudiziari Con conseguenti errori di trattamento; non applicazione delle restrizioni alla comunicazione e diffusione, comunicazione di dati a persone che non ne hanno diritto; cattiva gestione dei diritti dell'interessato nel caso li voglia far valere; errore materiale in buona fede, etc.
- **Incuria-Negligenza** : Disapplicazione delle istruzioni impartite per prevenire o ridurre i rischi. Cattiva gestione dell'eliminazione dei documenti, dei CD e floppy

disk da cestinare; faciloneria nel custodire la posta in arrivo e in partenza e durante spostamenti e consegne; cattiva gestione delle password e della loro segretezza, etc.

- **Imprudenza** : documenti cartacei lasciati sui tavoli o comunque in posizione tale da essere visti da chi non è autorizzato; documenti fatti circolare senza che siano in busta chiusa; esecuzione di fotocopie di documenti delicati sotto gli occhi di estranei; monitor lasciato visibile a estranei; computer abbandonato acceso senza screensaver [=immagine salvaschermo] comandata da password; documenti o dischi di computer lasciati dove facilmente sottraibili; cassette e contenitori non chiusi a chiave; stanze ad accesso selezionato o controllato non chiuse a chiave quando non presidiate; persone non autorizzate lasciate entrare in tali stanze, etc.
- **Carenza di consapevolezza e sottovalutazione della gravità del rischio** : l'incaricato non comprende la possibile rovinosità della non puntuale esecuzione del backup (=copia di sicurezza dei dati), dell'aggiornamento dell'antivirus, dell'aggiornamento della sicurezza del sistema operativo e dei programmi, di tenere attivo il firewall (=filtro anti-intrusione), etc.
- **Comportamenti sleali o fraudolenti** : sono sempre possibili, l'unica prevenzione è la vigilanza, nonché far ben comprendere che si può trattare di reati penali e che si può essere chiamati a risarcire i danni morali e materiali.

B - Rischi dei locali utilizzati (causati da possibili eventi distruttivi naturali o artificiali o dovuti ad incuria)

E' il rischio dipendente dall'esposizione dei locali ad eventi distruttivi, casuali o dolosi. Si prenda in considerazione come punto di riferimento la seguente casistica.

- Distruzione o perdita di dati in conseguenza di eventi naturali imprevedibili (terremoti, allagamenti, fulmini).
- Distruzione o perdita di dati a seguito di incendio (è il rischio principale connesso alla presenza di molta carta e di dispositivi elettrici). Incendi modesti producono fuliggine che rovina irrimediabilmente i computers. Uso di strumenti impropri per spegnere un inizio d'incendio, che creano danni ai dispositivi elettronici o ai supporti elettronici. Danneggiamento da calore di strumenti elettronici contenenti dati o dei dischi contenenti copie di backup (=salvataggio) dei dati
- Sbalzi di corrente e sovratensioni, fulmini: possono rovinare le apparecchiature elettroniche e far perdere i dati in memoria.
- Allagamento locale o infiltrazione d'acqua, che può rovinare documenti cartacei o apparecchiature elettroniche o creare problemi all'impianto elettrico.
- Errori umani nella gestione della sicurezza fisica (esempio: gettare mozziconi di sigarette nel cestino, dimenticare di spegnere i dispositivi che vanno spenti, uso di prolunghe inadatte, fili elettrici inadeguati, uso di moltiplicatori di presa, spine con carico di corrente eccessivo rispetto alla loro portata o coperte di polvere, ecc.).

C - Rischi dei locali utilizzati (legati all'accesso non autorizzato)

I rischi riguardano sia l'orario di lavoro (accessi di dipendenti e fornitori non autorizzati), sia le restanti ore della giornata e i giorni festivi (accessi di estranei, ma anche di

dipendenti comunque in servizio; e inoltre di manutentori e fornitori non autorizzati e/o lasciati senza controllo a vista).

- Sottrazione di password segrete.
- Sottrazione di documenti o di copia di essi. Furto di informazioni o danneggiamento degli strumenti elettronici o dei dati.
- Furto di strumenti elettronici contenenti dati.
- Consultazione di documenti riservati da parte di persone estranee o comunque non autorizzate. Consultazioni di archivi elettronici di computer da parte di persone estranee o comunque non autorizzate. Visione fortuita di dati riservati su carta o su computer.
- Atti vandalici che danneggiano i supporti dei dati (documenti, dischi, nastri, computers), in orario diverso da quello di lavoro.
- Atti deliberati di cancellazione di dati per eliminare informazioni sgradite o per favorire o danneggiare qualcuno, in orario diverso da quello di lavoro. Atti deliberati di modificazione di dati per favorire o danneggiare qualcuno.

D - Rischio guasti tecnici hardware, software, supporti (CD, dischetti, nastri, ecc.)

- Usura fisica o guasto di una componente hardware che blocca il funzionamento del computer singolo o del server da cui dipende una rete di computers (spesso dovuta alla mancata manutenzione regolare, in particolare dei dispositivi di raffreddamento); eccessivo degrado degli strumenti, che crea frequente e potenzialmente totale indisponibilità degli stessi.
- Guasto dei dischi fissi o dei CD o di altri supporti di registrazione, che divengono illeggibili (sbalzi di corrente, spegnimento improvviso o inappropriato del computer, polvere, strisci, deformazioni).
- Virus, worms (=vermi), Trojan Horses (=cavalli di Troia) o altri programmi maligni che impediscono il funzionamento del computer, cancellano dati, ecc.
- Perdita di dati dovuta a sbalzi di corrente elettrica o a improvvisa mancanza di essa.

E - Rischio penetrazione nei computers e nelle reti di comunicazione

- Accesso non autorizzato da parte di terzi – interni o esterni all'azienda o ente – mediante uso abusivo di credenziali di autenticazione, allo scopo di danneggiare, consultare o sottrarre dati.
- Intrusione per via telematica di hackers (= esperti di informatica che per via informatica entrano nei computers per curiosità o malinteso senso della sfida o per scopo di lucro, comunque con intento malevolo): possono farlo sfruttando falle nella sicurezza dei programmi o dei comportamenti degli operatori e potenzialmente rubare informazioni, compiere operazioni riservate agli addetti, modificare dati, cancellarli ed altro.
- Fuga informatica di notizie, tramite programmi che spediscono automaticamente

ad altri computers informazioni (spyware, virus, cookies); questi programmi vengono inoculati soprattutto in occasione della visita a certi siti web; i cookies sono relativamente poco pericolosi, in quanto dovrebbero servire solo ad aiutare un sito web a servire meglio le richieste.

- Virus o altro programma maligno che inviano i dati all'indirizzo di posta elettronica programmato dall'autore o agli indirizzi di posta elettronica registrati in computer.
- Accesso a zone protette del computer da parte di Incaricati che non ne hanno l'autorizzazione per quel livello (causa mancanza di protezione o insufficienza della stessa).
- Nel caso di reti aperte al pubblico, accesso di altri utenti a livelli non consentiti (causa mancanza di protezione o insufficienza).
- Errori umani nell'attivazione degli strumenti di protezione.

Obblighi del titolare contro i rischi individuati

Valutazione accurata

In pratica nel DPS il Titolare deve valutare per ciascuno dei rischi la **gravità** e il **grado di probabilità dell'evento**. Poi deve indicare le **contromisure già adottate e quelle ulteriori eventualmente previste**. Quindi, leggendo questa parte del DPS, **ogni Incaricato potrà conoscere i rischi e le misure di sicurezza poste in essere, in modo da applicarle consapevolmente e rispettarle**.

Adozione immediata di certe misure, progettazione di ulteriore misure

Alla luce dei fattori di rischio e delle aree individuate, si devono implementare misure di sicurezza di due tipi.

1) Le cosiddette **misure minime di sicurezza**, cui tutti sono tenuti sotto minaccia di seria sanzione penale. In pratica il ragionamento è che gestire dati personali altrui è un'attività di per sé pericolosa per gli interessati e quindi si è autorizzati a farlo solo rispettando determinate regole di sicurezza (in questo senso è assimilato dal Codice a qualsiasi altra attività pericolosa).

2) **Ulteriori misure di sicurezza**, in relazione anche alla gravità del rischio. Oltre alle regole minime, c'è l'obbligo di migliorare progressivamente la sicurezza con misure ulteriori, da valutare caso per caso.

Una misura di sicurezza può consistere in uno strumento elettronico di allarme o di rimedio a certi rischi, in apparati di prevenzione o protezione, in misure organizzative e in attività formative per la sensibilizzazione e preparazione degli addetti.

Le misure di sicurezza vanno descritte nel Documento Programmatico sulla Sicurezza sia quando sono state già attuate, sia come progetto da realizzare nel tempo.

Misure minime da adottare

Ogni Titolare del trattamento è tenuto ad adottare almeno le cosiddette "misure minime di sicurezza" individuate negli artt. 22 e da 31 a 36, volte ad assicurare un livello minimo di protezione dei dati personali. Il Codice così definisce le "misure minime": il complesso delle misure tecniche, informatiche, organizzative, logistiche [qualcuno interpreta: "logiche"] e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi sopra elencati.

Il Codice privacy ha un importantissima parte costituita dall'Allegato B, che detta le misure minime (=sotto tale livello non si può scendere senza commettere reato penale!).

La mancata adozione delle misure minime di sicurezza comporta una sanzione penale e la responsabilità civile per eventuali danni a un Interessato (risarcimento danni materiali e morali).

Misure minime per i trattamenti mediante computer o strumenti elettronici

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

Accesso al computer solo mediante autenticazione informatica: un nome-utente individuale (pubblicamente noto) e una password individuale segreta, conosciuta solo dalla persona che la utilizza (oppure altro sistema più efficace di identificazione, ad esempio, rilevazione elettronica delle impronte digitali, ecc.). Nel caso dell'uso della password, il nome-utente rimane identico nel tempo, mentre la password va modificata periodicamente (6 mesi, ma 3 se si tratta di dati sensibili o giudiziari). La password deve rispondere certi requisiti di sicurezza.

Un programma antivirus periodicamente aggiornato che impedisca ai programmi malevoli di fare danni o mandare dati a terzi.

Adozione di procedure per la custodia di copie di sicurezza (il cosiddetto backup, da fare almeno ogni 7 giorni), il ripristino della disponibilità dei dati e dei sistemi informatici entro 7 giorni in caso di guasto del computer o furto ecc...

Tenuta di un aggiornato "documento programmatico sulla sicurezza" [chiamato DPS], che all'inizio descrive lo stato iniziale del sistema e le misure adottate e da adottare e poi viene aggiornato annualmente con miglioramenti ulteriori della sicurezza.

I CD e floppy disk devono essere protetti affinché non siano rubati o usati per trattamenti non consentiti; se vengono dismessi, devono essere distrutti o formattati prima di assegnarli ad altri Incaricati.

Un progetto di formazione adeguata del personale ai vari livelli per applicare il Codice Privacy mediante corsi, letture, riunioni, ecc.

Misure minime per il trattamenti cartacei

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

Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito agli Incaricati. In pratica, nelle nomine degli Incaricati e dei Responsabili va indicato inizialmente quali banche dati e quali dati possono trattare. Questa individuazione va verificata periodicamente e se se cambia qualcosa nell'organizzazione, le nomine vanno aggiornate di conseguenza, indicando quali banche dati e quali dati possono trattare dai Responsabili e Incaricati chiamati in causa.

Previsione di procedure per un'ideale custodia di atti e documenti affidati agli Incaricati per lo svolgimento dei relativi compiti. Significa: verifica che i dati siano custoditi in cassetti chiudibili o contenitori chiudibili o stanze-archivio chiudibili; verifica che i predetti sistemi di custodia siano idonei rispetto al grado di importanza del dato per la privacy (i dati sensibili e giudiziari devono essere ovviamente più protetti).

Sicurezza da furti, vandalismi e intrusioni: presenza o meno di antifurto, qualità dei serramenti ed infissi, qualità delle serrature, eventuale guardiania. Infine,

Sicurezza da eventi che potrebbero minacciare l'integrità dei dati (incendi, alluvioni, perdite d'acqua ed altri eventi).

Previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli Incaricati. Significa che vanno impostate procedure che garantiscano il controllo dell'accesso alle chiavi, riservandolo effettivamente a chi è autorizzato ad accedere ai dati.

LEZIONE 7

Nasce per l'Interessato il diritto di accesso ai propri dati personali

L'Interessato (persona o Ente o associazione ecc.) ha diritto di conoscere i dati che lo riguardano e in certi casi di intervenire su di essi per farli cancellare, modificare o aggiornare. Detti diritti vanno illustrati per esteso nell'informativa.

Da notare che si tratta di cosa diversa dal diritto di accesso ai documenti amministrativi sancito dalla legge 241.

In sostanza, l'Interessato ha diritto di ottenere da Aziende, Società, Associazioni, Enti ed esercenti attività economiche o professionali la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati. E in certi casi di modificarli o cessare di trattarli.

La richiesta va presentata di persona o trasmessa anche mediante lettera raccomandata, telefax o posta elettronica, al titolare o al responsabile, anche per il tramite di un suo incaricato. **La controparte ha l'obbligo di fornire riscontro idoneo e senza ritardo, con una risposta comprensibile e senza costi.** Infatti il Titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:

ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;

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

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

Cosa il Cittadino ha diritto di conoscere

In particolare il Cittadino ha diritto di conoscere da chi detiene suoi dati personali:

l'origine dei dati personali;

le finalità e modalità del trattamento;

la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

gli estremi identificativi del titolare e dei responsabili del trattamento di dati;

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.

Cosa il Cittadino ha diritto di ottenere

Il Cittadino ha diritto:

➤ all'aggiornamento, alla rettificazione ovvero, quando vi ha interesse, all'integrazione

dei dati.

- alla cancellazione, alla trasformazione in forma anonima o al 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;
- all'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.

Il Cittadino, inoltre, ha diritto di opporsi, in tutto o in parte:

al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Accesso a documenti amministrativi degli enti pubblici

Attenzione: stiamo parlando dell'accesso di qualcuno che è diverso dall'Interessato. Infatti l'Interessato ha già nel Codice il pieno e incondizionato diritto di accesso ai propri dati. Il diritto di accesso a documenti amministrativi, detenuti da Enti Pubblici e contenenti dati personali resta consentito e disciplinato dalla legge 7 agosto 1990 n. 241, anche per ciò che concerne i Dati Sensibili e Giudiziari (con l'eccezione dei dati idonei a rivelare lo stato di salute o la vita sessuale per i quali va fatta apposita valutazione). Talvolta può crearsi un conflitto tra il diritto di accesso di qualcuno ai dati personali di un'altra persona e il dovere di riservatezza sui dati a cui un Ente Pubblico Titolare è tenuto. Il titolare risolve il conflitto compiendo una valutazione comparata dei valori e delle motivazioni che si contrappongono (sull'argomento esistono testi specializzati).

Chi deve applicare il Codice Privacy

Qualunque ditta, ente, lavoratore autonomo, libero professionista, associazione. **Obblighi più forti se, nell'ambito dell'attività, viene utilizzato almeno un computer e se sono trattati Dati Sensibili o Giudiziari.** Nel caso di strutture nazionali, l'obbligo ricade sulla sede locale se essa ha autonomia organizzativa.

Nascono nuovi doveri per Aziende, Società, Associazioni, Enti, Esercenti attività economiche o professionali ... e anche per il Cittadino

Il Codice Privacy disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato:

da chiunque è stabilito in un luogo comunque soggetto alla sovranità italiana;

dallo straniero proveniente da fuori UE che impiega, per il trattamento dei dati personali, strumenti situati nel territorio italiano.

Il Codice Privacy si applica parzialmente anche al privato cittadino

Il Codice si applica al **trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali** solo quando i dati siano destinati ad una **comunicazione sistematica o alla diffusione**.

Si applicano in ogni caso a tutti, anche ai privati, le disposizioni in tema di responsabilità e di sicurezza dei dati di cui all'art. 15 (procedura speciale favorevole al danneggiato per rispondere dei danni materiali e morali) e art. 31, che riportiamo: <<**Art. 31. Obblighi di sicurezza**
1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.>>. In sostanza, **anche il privato risponde dei danni causati, anche in buona fede, dalla cattiva custodia, dallo smarrimento di dati personali altrui, nonché da comunicazioni o diffusions scorrette o illecite.**

Perché il Codice Privacy e perché così severo ?

Il Codice Privacy, reso obbligatorio dall'Unione Europea, ha una giustificazione sacrosanta : tenta di opporre una diga alle incombenti minacce del *moloch* della società informatizzata e globalizzata. Ormai quasi ogni cosa che l'individuo fa lascia automaticamente una traccia in un computer. A volte sono informazioni banali, altre volte molto delicate. Ma anche le informazioni in apparenza banali, se collegate in modo sistematico a tutte le altre, possono rivelare aspetti molto intimi di una persona, comprese le sue idee.

Immaginate che queste informazioni su ogni individuo vengano accumulate sistematicamente per anni, registrandole in computers di diversi enti pubblici o società private e che i diversi computer possano mettere in comune i loro archivi, creando **super-archivi o reti di archivi interconnessi tramite computers che potrebbero accedere a tutti i dati**. Allora, chi controllasse i computer potrebbe sapere quasi tutto su ogni persona, anche le cose più intime e riservate, comprese le sue idee, e potrebbe servirse-ne per ridurre sia la libertà dell'individuo sia la libertà del mercato.

Tutto questo da qualche anno è tecnicamente possibile e in parte si cominciava a fare schedando le persone su diversi parametri. Per esempio, esiste un programma per il centralino telefonico di grandi società che assegna i tempi d'attesa in base al reddito del intestatario del numero telefonico: chi è più povero aspetta di più o gli cade la linea.

Il Codice Privacy vuole, appunto, impedire: la raccolta non autorizzata di dati personali, il loro accumulo nel tempo e la loro comunicazione ad altri se non autorizzata dalla legge.

Pertanto le nuove regole privacy impongono che l'acquisizione, la conservazione, la comunicazione di dati possano avvenire soltanto quando siano strettamente indispensabili ed espressamente autorizzate dalla legge o dall'Interessato (in questo caso, però, limitatamente alle operazioni da lui richieste). Inoltre, impongono che i dati possano essere conservati esclusivamente per il tempo necessario ad eseguire le operazioni richieste dall'Interessato e poi vadano cancellati (o distrutti, se sono documenti o nastri o dischi ecc.)

Per ottenere che queste regole siano rispettate sono state previste multe salatissime e veri e propri reati di codice penale, puniti con l'arresto.

E' evidente la validità di questo obiettivo nei confronti delle grandi organizzazioni che effettivamente potrebbero minacciare la privacy dell'individuo, tant'è che ci sono regole particolari, ancora più severe, per le società di telecomunicazioni, per le assicurazioni, le banche e gestori del credito, ecc..

Tuttavia il guaio è che la legge italiana prevede che queste regole così rigide e queste sanzioni tanto pesanti siano applicate anche ai piccoli enti e ditte, che comunque non sono altrettanto pericolosi per la privacy. Ciò sembra francamente esagerato e fuori misura. Comunque, poiché la situazione è questa, nessuno deve prendere sottogamba il Codice Privacy, anche se gli sembra che i dati da lui gestiti siano innocenti. Infatti se arriva un controllo o una denuncia anche malevola, le sanzioni sono – ripetiamo – esagerate e troppo pesanti per le infrazioni modeste (si pensi che la più piccola multa concretamente applicabile è di ben € 6.000 !).

Al Dirigente scolastico

Oggetto: attestazione della formazione obbligatoria relativamente al DLgs 196/2003 di cui all'Allegato B - regola 19.6

Argomento: **Compendio di livello base**

	Questionario (barrare le caselle corrispondenti alle risposte esatte)	S I	N O
1	Nel linguaggio del Codice Privacy, chi fra questi è un "TITOLARE" ?		
1-a	La Scuola Media "De Amicis" di Milano		
1-b	Il Comune di Roma		
1-c	La Provincia di Potenza		
1-d	Il Dirigente Scolastico (Preside) della Scuola Media "Pascoli" di Roma		
2	Nel linguaggio del Codice Privacy, chi fra questi è un INTERESSATO?		
2-a	L'Ente o la ditta di cui si trattano di dati		
2-b	Qualunque persona interessata ai dati trattati		
2-c	La persona di cui si trattano i dati		
2-d	L'Ente o la persona che tratta i dati		
3	Il codice bancomat è un dato sensibile ?		
4	La domanda di astensione dal lavoro per gravidanza è un dato sensibile ?		
5	Se un dipendente chiede un permesso sindacale è un dato sensibile?		
6	Per un Ente Pubblico ci sono limitazioni alla comunicazione di dati comuni ad altri Enti Pubblici ?		
7	La domanda di permesso sindacale è un dato sensibile?		
8	Esporre dei dati all'albo è una comunicazione ?		
9	Per un Ente Pubblico ci sono limitazioni a trattare dati sensibili?		
10	Si può eseguire qualche trattamento di dati personali senza essere stato nominato Incaricato o Responsabile ?		

Il sottoscritto _____

Qualifica _____

dichiara di aver letto con attenzione in ogni sua parte il manuale di *Pagine-scuola/PaginePA*, di livello base, composto di 34 pagine, di aver risposto al questionario sopra riportato e di essere stato informato che sono disponibili ulteriori dispense di approfondimento per le tematiche specificamente connesse con il proprio ruolo sul server di rete (cartella Privacy), nonché, è disponibile per la consultazione il Documento Programmatico sulla Sicurezza, in particolare nella parte relativa alle misure di sicurezza.

In fede

Data: ____ . ____ . 200__ firma _____

Per un aggiornamento più dettagliato e continuo visitare il sito internet
www.battaglinivenosa.it