Commento breve al D.LGS.VO N. 196/2003.
Codice in materia di protezione dei dati personali

SOMMARIO: Premessa. La tutela della riservatezza in Italia ante legge n. 675/96. Origine ed evoluzione del concetto di privacy in Italia. I principi generali. Cap. II - Parte I Disposizioni generali Titolo I Principi Generali. Art. 1 Diritto alla protezione dei dati personali. Art. 2 Finalità. Art. 3 Principio di necessità nel trattamento dei dati. Art. 4 Definizioni. Art. 5 Oggetto ed ambito di applicazione. Art. 6 Disciplina del trattamento. Cap. III – Titolo II Diritti dell'interessato. Art. 7 Diritto di accesso ai dati personali ed altri diritti. Art. 8 Esercizio dei diritti. Art. 9 Modalità di esercizio. Art. 10 Riscontro all'interessato. Cap. IV – Titolo III Regole generali per il trattamento dei dati. Capo I Regole per tutti i trattamenti. Art. 11 Modalità del trattamento e requisiti dei dati. Art. 12 Codici di deontologia e di buona condotta. Art. 13 Informativa. Art. 14 Definizione dei profili e della personalità dell'interessato. Art. 15 Danni cagionati per effetto del trattamento. Art. 16 Cessazione del trattamento. Art. 17 Trattamento che presenta rischi specifici. Cap. V Regole ulteriori per i soggetti pubblici. Art. 18 Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici. Art. 19 Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari. Art. 20 Principi applicabili al trattamento di dati sensibili. Art. 21 Principi applicabili al trattamento di dati giudiziari. Art. 22 Principi applicabili al trattamento di dati sensibili e giudiziari. Capo III Regole ulteriori per privati ed enti pubblici economici. Art. 23 Consenso. Art. 24 Casi nei quali può essere effettuato il trattamento senza consenso. Art. 25 Divieti di comunicazione e diffusione. Art. 26 garanzie per i dati sensibili. Art. 27 Garanzie per i dati giudiziari. Titolo IV Soggetti che effettuano il trattamento Art. 28 Titolare del trattamento. Art. 29 Responsabile del trattamento. Art. 30 Incaricati del trattamento. Titolo V Sicurezza dei dati e dei sistemi. Art. 31 obblighi di sicurezza. Art. 32 Particolari titolari. Art. 33 Misure minime. Art. 34 Trattamenti con strumenti elettronici. Art. 35 Trattamenti senza l'ausilio di strumenti elettronici. Art. 36 Adeguamento Disciplinare tecnico in materia di misure minime di sicurezza.Sistema di autorizzazione. Il trattamento dei dati senza l'ausilio di strumenti elettronici. Il calendario con le date relative all'adozione delle misure di sicurezza. Titolo VI Adempimenti. Art. 37 Nitificazione del trattamento. Art. 38 Modalità di notificazione. Art. 39 Obblighi di comunicazione. Art. 40 Autorizzazioni generali.art. 41 Richieste di autorizzazione. Titolo VII Trasferimento dei dati all'estero. Art. 42 Trasferimenti all'interno della Unione europea. Art. 43 Trasferimenti consentiti in paesi terzi. Art. 44 Altri trasferimenti consentiti. Parte II Disposizioni relative e specifici settori. Titolo IV Trattamenti in ambito pubblico. Capo I Accesso a documenti amministrativi Art. 59 Accesso ai documenti amministrativi. Art. 60 Dati idonei a rivelare lo stato di salute e la vita sessuale. Titolo V Trattamento di dati personali in ambito sanitario Capo I principi generali. Art. 75 Ambito applicativo. Art. 76 Esercenti professioni sanitarie e organismi sanitari pubblici. Art. 77 Casi di semplificazione. Art. 78 Informativa del medico di medicina generale o del pediatra. Art. 79 Informativa da parte di organismi sanitari. Art. 80 Informativa da parte di altri soggetti pubblici. Art. 81 Prestazione del consenso. Art. 82 Emergenze e tutela della salute e dell'incolumità fisica. Art. 84 Comunicazione di dati all'interessato.- art. 85 Compiti dell Servizio sanitario Nazionale. Art. 86 Altre finalità di rilevante interesse pubblico. Artt. 87,88,89 Le prescrizioni mediche: medicinali a carico e non del SSN e casi particolari. Art. 90 Trattamento dei dati genetici

Autore: Dott. Giovanni Modesti Referente Aziendale per la Privacy c/o AUSL di Pescara

e donatori di midollo osseo. Art. 91 Dati trattati mediante carte. Art. 92 Cartelle cliniche.art. 93 Certificato di assistenza al parto. Art. 94 Banche di dati, registri e schedari in ambito sanitario. Titolo VIII Lavoro e previdenza sociale. Capo I Profili generali. Art. 111 Codice di deontologia e di buona condotta. Capo III Divieti di controllo a distanza e telelavoro. Art. 114 Controllo a distanza. Art. 115 Telelavoro e lavoro a domicilio. Titolo X Comuinicazioni Elettroniche Capo I Servizi di comunicazione e lettronica. Art. 132 Conservazione di dati di traffico per altre finalità. Ca<po III Video sorveglianza. Art. 134 Codice di deontologia e di buona condotta.Parte III Tutela dell'interessato e sanzioni. Art. 141 Forme di tutela. Art. 142 Proposizione dei reclami. Art. 143 Procedimento per i reclami. Art. 144 Segnalazioni. Art, 145 Ricorsi. Art. 146 Interpello preventivo. Art. 147 Presentazione del ricorso. Art. 148 Inammissibilità del ricorso. Art. 149 Procedimento relativo al ricorso. Art. 150 provvedimenti a seguito del ricorso. Art. 151 Opposizione. Art. 152 Attività giudiziaria ordinaria. Titolo II L'Autorità.Capo I Il Garante per la protezione dei dati personali. Art. 153 Il Garante. Art. 154 Compiti. Capo II L'Ufficio del garante Artt. 155 e 156 Principi e ruolo organico e personale. Capo III Accertamenti e controlli. Art. 157 Richiesta di informazioni e di esibizione di documenti. Art. 158 Accertamenti. Art. 159 Modalità. Art. 160 Particolari accertamenti. Titolo III Sanzioni. Capo I Violazioni amministrative. Art. 161 Omessa o inidonea informativa all'interessato. Art. 162 Altre fattispecie. Art. 163 Omessa o incompleta notificazione.art. 164 Omessa informazione o esibizione al garante. Art. 165 Pubblicazione del provvedimento del Garante. Art. 166 Procedimento di applicazione. Capo II Gli illeciti penali. Art. 167 Trattamento illecito dei dati. Art. 168 Falsità nelle dichiarazioni e notificazioni al Garante. Art. 169 Misure di sicurezza. Art. 170 Inosservanza di provvedimenti del garante. Art. 17 1 Altre fattispecie. Art. 172 Pene accessorie. Titolo IV Disposizioni modificative, abrogativem transitorie e finali. Capo I Disposizioni di modifica. Artt. 173-186 L'entrata in vigore del Codice e l'incidenza sulla normativa previdente, con particolare evidenza all'art. 177 Disciplina anagrafica, dello stato civile e delle liste elettorali e all'art. 178 Disposizioni in materia sanitaria. Capo II Disposizioni transitorie Art. 180 Misure di sicurezza. Art. 181 Altre disposizioni transitorie.

Premessa

In Europa la privacy[1] comincia ad assumere il significato moderno di diritto fondamentale della persona umana alla fine del '700, allorché Lord Chatham – nel 1766 – pronunciò nel Parlamento inglese, in un dibattito sull'uso delle garanzie, la seguente frase: " Il più povero degli uomini può, nella sua casetta lanciare una sfida alla… corona. La casetta può essere fragile,…ma il re d'Inghilterra non può entrare..". La privacy nasce dalla capacità della persona di opporsi alla forza della Corona e come conseguenza ne deriva la determinazione di precisi limiti all'azione dello Stato e della sfera pubblica nei confronti dell'individuo. Il diritto di privacy è quindi il diritto dell'individuo di "to be let alone", di essere lasciato solo, è la pretesa giusta dell'individuo di determinare in che misura egli desidera condividere parte di sé con gli altri. E' anche il diritto dell'individuo di controllare la diffusione dell'informazione circa se stesso.

Nel **1890** a Boston un avvocato di successo, stanco di leggere sui giornali locali le vicende della moglie si rivolse ad un giudice invitandolo a studiare il problema. Insieme pubblicarono il famoso saggio The right to privacy. Alla privacy fu presto riconosciuta il valore di diritto fondamentale alla pari della proprietà su cui era modellato.

La tutela della riservatezza venne poi sancita solennemente dall'art. 12 della **Dichiarazione Universale dei diritti dell'uomo** che vietava "l'arbitraria interferenza con la riservatezza". In seguito, la **Convenzione europea sui diritti dell'uomo**, del 1950, all'art. 8, recita che "ogni persona ha diritto al rispetto della sua vita privata e familiare" e all'art. 10 precisa che la stessa libertà di espressione incontra, tra i suoi limiti, il divieto di divulgare "informazioni confidenziali".

In Europa nei primi anni settanta, nascono le leggi sulla tutela della riservatezza in Svezia (1973), nella Germania Federale (1977), in Austria, Danimarca, Francia e Norvegia (1978).

---

[1] Bibliografia: **A.Ccacciari**, La tutela della riservatezza dei dati personali nelle pubbliche amministrazioni; 2004, Se; **M.De Giorni e A. Lisi**, Guida al Codice della Privacy,2003, Simone; **G. Elli e R. Zallone**, Il nuovo Codice della privacy,2004, Giappichelli; **A. Biasiotti**, Il nuovo testo Unico sulla privacy, 2003, Informa; **U. rametto, B.Rametto Freddi,** Privacy & Sicurezza, 2003, Informa.**G. Pomante,** Riservatezza e nuove tecnologie dell'informazione; Violazione della privacy: come proteggersi?; Tecnologie aziendali e loro uso privato:: che cosa dice il Codice; Sorvegliare, controllare, identificare mediante video: profili giuridici; Riservatezza e trattamento: la parola all'avvocato; Frode informatica, la soluzione arriva dall'articolo 640 ter; la nuova privacy: esattezza e pertinenza del dato trattato; saggi tratti da www.pomante.com; **C. Bonaria, Quattro passi preliminari per approntare il "DPS",** tratto da WWW.dossier.duke.it; **E. Aggrazio,** Guida pratica per la stesura del Documento Programmatico per la Sicurezza, tratto da WWW. dossier.duke.it; **L. Baffigo,** Il sistema o l'architettura di sicurezza, in Diritto &Pratica del Lavoro, n. 23/04; **A. Bellavista,** Protezione dei dati personali nel rapporto di lavoro, Ipsoa; **G. Carozzi,** Gli adempimenti dei titolari nei confronti dei clienti-utenti, in Diritto & Pratica del Lavoro n. 22/04; **G. Carozzi,** Sanzioni e contenzioso, in Diritto & Pratica del Lavoro n. 25;/04; **S. Cimini,** Diritto di accesso e riservatezza: il legislatore alla ricerca di nuovi equilibri; 2005, Giappichelli; **R. Di Pietro,** Il piano della sicurezza e le responsabilità della privacy**;** 2004**; G. Elli,** Trattamento dei dati: ruoli e responsabilità, 2004, in Diritto & Pratica del Lavoro; **N. Lugaresi,** Protezione della privacy e protezione dei dati personali: i limiti dell'approccio comunitario; in Giustizia Amministrativa, 2004; **A. Manna,** Prime osservazioni sul Testo Unico in materia di protezione dei dati personali: profili penalistici;2004; **G. Tonelli,** Il delitto di accesso abusivo a sistemi informatici o telematici con particolare riferimento alla tutela dei dati personali, 2005;

Autore: Dott. Giovanni Modesti Referente Aziendale per la Privacy c/o AUSL di Pescara

Il **28 gennaio 1981** viene approvata a Strasburgo, la Convenzione per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale.La Convenzione del Consiglio d'Europa ribadì la necessità di assicurare il diritto alla riservatezza degli individui e confermò i limiti di ingerenza della P.A. ai casi specificamente previsti da una legge.
Da ultimo, con Direttiva sulla privacy del 24 ottobre 1995, n. 95/46 CE, adottata dal Parlamento europeo, si garantì, all'art. 1, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata.

La Carta dei diritti fondamentali dell'U.E. del 7 dicembre 2000, così recita all'art. 7 (Rispetto della vita privata e della vita familiare): "ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni"; mentre all'art. 8 (Protezione dei dati di carattere personale): " Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

La tutela della riservatezza in Italia ante legge n. 675/96

L'Italia[2] è uno dei firmatari della Convezione di Strasburgo, pur non avendo nel suo ordinamento una previsione normativa vera a tutela della riservatezza. La Costituzione non dedica alcuna norma specifica alla tutela della riservatezza in quanto tale, anche se vari principi si possono individuare nelle norme poste a tutela del domicilio (art. 14), della libertà e segretezza della corrispondenza (art. 15), ecc.

E' stata quindi la giurisprudenza ad individuare il fondamento giuridico della privacy quale diritto costituzionalmente tutelato e lo ha fatto con la sentenza della Corte di Cassazione, n. 2129 del 27 maggio 1975, nella quale si sancisce definitivamente la riservatezza come diritto costituzionalmente tutelato in base, tra l'altro, all'art. 2 della Costituzione

L'Italia però restava l'unico Paese firmatario della Convenzione che alla stessa non aveva dato attuazione.

Nel nostro ordinamento vennero identificate altre norme poste a tutela della riservatezza.

Nel **1970** il diritto alla privacy ha il suo primo riconoscimento legislativo, in Italia, nella Carta dei Diritti dei Lavoratori dove l'articolo 8 recita che è fatto divieto al datore di lavoro di effettuare indagini ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, sulle opinioni politiche, religiose o sindacali dei lavoratori.
Non è da escludere che l'origine del diritto di privacy sia legata al diritto di proprietà ma oggi è ormai acquisito che la privacy è una caratteristica connessa alla dignità della persona. Per

[2] Riferimenti normativi: **Direttiva 95/46/CE, del 24.10.1995**, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati; **L. 31 dicembre 1996 n. 675,** Tutela delle persoine e di altri soggetti rispetto al trattamento dei dati personali..**Lgs. 30 giugno 21003, n. 196 –** Codice in materia di protezione dei dati personali; **D.Lgs. 30 luglio 1999, n. 281 –**Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica; **D.P.R. 28 dicembre 2000, n. 445 –** Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

potere vivere con dignità e rispetto di sé, la persona deve riuscire a determinare quali e quante informazioni sul proprio conto siano divulgate agli altri. Noi siamo le nostre informazioni: siamo passati dall'habeas corpus all'habeas data. La nostra identità è anche affidata al modo in cui queste informazioni vengono raccolte, trattate, collegate, fatte circolare.

Nel **1972**, il Mulino pubblicò un libro dal titolo "Elaboratori elettronici e controllo sociale" con il quale Stefano Rodotà invocava una adeguata normativa per tutelare il cittadino dalle banche dati che si affacciavano sempre più minacciose per la libertà individuale. L'autore concepì un fascio di tutele non più in chiave di difesa "proprietaria" ma di controllo sul flusso di informazioni che venivano raccolte. Un sistema basato, in parte, sulla necessità del consenso – in alcuni casi non necessario, in altri insufficiente – e sulla liceità del trattamento solo ricorrendo determinate condizioni. Il mito del consenso può essere ingannevole in quanto può nascondere una situazione di disparità che, aggiungeva Rodotà, " vanifica la proclamata uguaglianza formale delle loro dichiarazioni di volontà". Il consenso, talvolta, può essere debole (e, quindi, da solo non bastevole): ad esempio quando per ottenere un prestito sono richiesti dati "sensibili". Prudente cautela è stata allora quella di avere previsto come necessaria anche l'autorizzazione del Garante che "conferma" il consenso degli interessati verificandone la rispondenza all'interesse primario alla riservatezza e dunque allo sviluppo della personalità che la Costituzione tutela quale diritto fondamentale e inviolabile della persona.

Origine ed evoluzione del concetto di privacy in Italia

In Italia la normativa sulla privacy arriva sulla spinta della Unione Europea, grazie a due normative:

il Trattato di Schengen che elimina i controlli alle frontiere ed assicura la libera circolazione delle persone, unitamente alle informazioni che le riguardano. Poiché uno dei principi chiave presenti in tutte le legislazioni europee in materia di tutela dei dati sancisce che il loro trasferimento da un paese all'altro presuppone che lo Stato ricevente abbia adottato misure di protezione adeguate e, comunque, paragonabili a quelle garantite nello Stato di origine, la mancanza in Italia di una legge sulla tutela dei dati personali le avrebbe impedito di fare parte del gruppo dei Paesi di Schengen.

La Direttiva n. 95/46, sulla tutela dei dati personali, che imponeva agli Stati membri il recepimento della stessa entro tre anni dalla sua entrata in vigore.

Questi due fatti hanno dato la spinta alla promulgazione della **Legge 675/96**, ora abrogata, che creava una normativa organica in materia di protezione della privacy, volta esplicitamente alla tutela della dignità, dei diritti e delle libertà fondamentali delle persone, riferendosi quindi a quelli che vengono definiti come "diritti inviolabili" delle persone umane, in particolare ai diritti alla riservatezza e all'identità personale. Entrambe le posizioni giuridiche sono state ribadite dal D.Lgs.vo n. 196/2003 che ha elevato la protezione dei dati personali a posizione giuridica autonoma e l'ha riconosciuta in capo a "chiunque". La protezione dei dati assurge essa stessa a diritto fondamentale della persona, sia fisica sia giuridica e si affianca alla riservatezza e all'identità personale.

La normativa in questione ha come scopo la protezione dei dati personali, definiti dalla stessa come *informazioni relative ad una persona (fisica o giuridica),* allo scopo di tutelare dette posizioni giuridiche che si qualificano, quali diritti fondamentali della persona umana. La posizione di indipendenza degli individui è stata tutelata attraverso il riconoscimento di "diritti della personalità", cioè di posizioni giuridiche attive che sono connaturate all'esistenza stessa delle persone. Si tratta di posizioni giuridiche attive consistenti nella pretesa a salvaguardare la propria esistenza da intromissioni non necessarie dell'Autorità statale, e sono

riconosciute ad ogni persona per il solo fatto di venire ad esistenza. La persona umana, in tutte le sue manifestazioni, deve essere protetta sia nei confronti della P.A. sia nei confronti di privati in virtù della esistenza di diritti fondamentali costituzionalizzati dall'art. 2 della Costituzione, che li "riconosce" e li "garantisce". I diritti fondamentali della persona sono legati all'esistenza stessa delle persone e preesistono allo stesso ordinamento e sono imprescrittibili. Essi non sono suscettibili di rinuncia, né gratuito né verso corrispettivo, se non nei limiti previsti dall'art. 5 c.c., con riferimento agli atti di disposizione del proprio corpo.

Il primo diritto fondamentale della persona umana è quello alla vita ed all'integrità fisica, da questo si è potuto evincere l'esistenza di un più generale diritto alla salute e al benessere psicofisico. Dal diritto alla propria immagine, normata dalla legge sul diritto di autore, si è ricavata l'esistenza di un generale diritto alla riservatezza, ad essere lasciati in pace, a tutela dalle intromissioni non gradite da parte di terzi. Dal diritto al nome, previsto dal c.c., l'interprete ha ricavato l'esistenza di un generale diritto all'identità personale, identificabile nel diritto ad essere riconosciuti nella vita sociale per sé stessi.

La protezione dei dati personali è tesa ad evitare intromissioni indesiderate nella propria vita privata, da un lato, e a garantire, dall'altro, che le operazioni di trattamento dei dati avvengano nel rispetto della veridicità delle informazioni relative a soggetti determinati. Nella vita sociale ed economica tale protezione non può essere assoluta poiché nessun individuo vive totalmente isolato. Occorre individuare strumenti che contemperino, da un lato, l'esigenza di tutela delle informazioni personali; dall'altro, la necessità che tali informazioni circolino per potere garantire lo sviluppo dei contatti e delle relazioni economiche e sociali necessarie per l'esistenza stessa della società. Poiché il dato personale, cioè l'informazione su qualunque circostanza riguardi la persona, è tutelato dall'ordinamento come un diritto fondamentale, per potere acquisire il dato personale di terzi, comunicarlo o collocarlo in un archivio, è necessario il consenso dell'interessato.

La **legge 3 febbraio 2003, n. 14**, recante "Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle comunità europee. Legge comunitaria 2002" delega al Governo- tra le altre cose - l'attuazione della direttiva comunitaria 2002/58/Ce del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali, entro 18 mesi, cioè entro il 30 giugno 2003. La direttiva, sopra richiamata, disciplina le comunicazioni elettroniche e lo fa assoggettando ad un unico quadro normativo i settori delle telecomunicazioni, dei media e delle tecnologie dell'informazione; prescindendo dal fatto che i dati personali siano utilizzati sulle reti telefoniche o sul web.

I principi generali

La struttura[3] Il codice, si compone di centottantasei articoli, più una serie di allegati, tra cui tre codici deontologici e un disciplinare sulle misure di sicurezza. Esso è diviso in tre parti.

[3] Lo schema seguito dal Codice per definire le regole applicabili nelle diverse circostanze si presenta articolato su tre livelli. Il primo è dato dalle "disposizioni generali" applicabili a qualunque trattamento, da chiunque effettuato sul territorio italiano. Il secondo è dato dalle "regole ulteriori" previste per diversificare il regime del trattamento dei dati che deve essere seguito distintamente dai soggetti pubblici e dai soggetti privati. Le "regole ulteriori" per i soggetti pubblici sono riportate negli articoli 18-22. il terzo livello è dato dalle "disposizioni specifiche" dettate per disciplinare l'attività di trattamento dei dati effettuato, nell'ambito di particolari settori di attività, sia pubblici che privati, che in funzione delle finalità perseguite,

La prima contiene le norme di carattere generale (art. 1 a 45), utili per qualsiasi trattamento di dati. Diritti e tutele sono collocati con evidenza all'inizio del Codice, facendo risaltare la disciplina di garanzia (art. 6). Al suo interno detta inoltre le regole "ulteriori" applicabili, da un lato, ai soli soggetti pubblici (artt. 18/46) e, dall'altro quelle applicabili ai privati, inclusi i Concessionari di pubblici servizi e degli enti pubblici economici..

Nella seconda parte, (artt. 46/140)si introducono i distinguo, in particolare quelli relativi all'utilizzo di dati personali nell'ambito della pubblica amministrazione, in quello giudiziario e in campo sanitario. La terza parte (artt. 141/186) contiene la tutela dei diritti e le sanzioni e spiega come tutelare la privacy quando il diritto d'accesso non ha dato i frutti sperati. In quei casi è possibile attivare il Garante o il giudice ordinario. Nella stessa parte del codice sono elencate anche le misure sanzionatorie da applicare nei confronti di chi utilizza i dati personali in maniera impropria.

Tutte le norme riunite sono di rango legislativo e ciò ha permesso di semplificare del 30% circa le norme vigenti.

I tre allegati che completano le disposizioni del Codice si compongono di:

Allegato A – Codici Deontologici;

Allegato B – Misure Minime di sicurezza;

Allegato C – Trattamenti in ambito giudiziario e di polizia.

La privacy europea. Il testo unico ha recepito parte dei contenuti della direttiva n. 2002/58/Ce, in particolare per quanto riguarda il c.d. meccanismo dell'opt-in: chi spedisce a un indirizzo di posta elettronica, fax, telefono o telefonino (con gli Mms) messaggi commerciali, deve preoccuparsi di acquisire il consenso del destinatario di quei messaggi.

Nel nuovo codice si assiste ad un ampliamento dell'ambito di applicazione rispetto al quadro comunitario: secondo la direttiva n. 95/46 i dati personali oggetto di applicazione della direttiva riguardano esclusivamente le persone fisiche, al contrario del nuovo codice italiano che all'art. 1 dispone che "chiunque ha diritto alla protezione dei dati personali che lo riguardano", specificando che per dato personale s'intende qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione.

Il codice sulla privacy non stabilisce un rinvio generale- riconoscendone la prevalenza- al diritto comunitario, ma lo afferma limitatamente a talune disposizioni come ad es. all'art. 13, comma 5, nel quale, in materia di informativa all'interessato, è stabilita l'inapplicabilità di alcuni obblighi per i dati "trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria".

Il diritto fondamentale alla privacy. Malgrado l'affermazione di un vero e proprio diritto alla privacy che tutela il valore della dignità della persona e la vita personale e familiare di un individuo e che quindi costituisce un diritto della personalità, si profila un'attenuazione della protezione dei dati a livello internazionale non solo a causa delle nuove tecnologie, ma soprattutto per esigenze connesse alla sicurezza nazionale e a motivi di ordine pubblico, con un rafforzamento e un ampliamento della conservazione dei dati senza limiti di tempo, prescindendo da ogni forma di consenso.

---

della delicatezza dei dati trattati (ad es. il servizio sanitario), presentano peculiarità tali da richiedere e giustificare norme ad hoc. Le disposizioni specifiche si aggiungono sia alle "disposizioni generali" applicabili a tutti i trattamenti, si alle "regole ulteriori" che differenziano la disciplina valida in ambito pubblico da quella valida in ambito privato, per integrarle o, solo ove espressamente previsto, per sostituirle o renderle inapplicabili nello specifico caso contemplato.

Parte I
DISPOSIZIONI GENERALI
TITOLO I
PRINCIPI GENERALI

Art. 1 Diritto alla protezione dei dati personali

Nel nuovo codice sulla privacy si assiste ad un ampliamento dell'ambito di applicazione rispetto al quadro comunitario: secondo la direttiva n. 95/46, così come interpretata dalla Corte di giustizia, i dati personali oggetto di applicazione della direttiva riguardavano esclusivamente le persone fisiche, al contrario del nuovo Codice italiano che in questo articolo 1 dispone che "chiunque ha diritto alla protezione dei dati personali che lo riguardano", specificando che per dato personale s'intende qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione.

Art. 2 Finalità

Punto di orientamento della intera normativa va considerato l'art. 2 della Costituzione. Ulteriori principi sono: la semplificazione (ovvero riduzione degli adempimenti e delle procedure), armonizzazione (cioè, previsione di incombenze e di tutele maggiormente omogenee rispetto al rango dei diritti da tutelare), ed efficacia (ovvero capacità del sistema di garantire un più elevato livello di osservanza dei principi della materia).

Art. 3 Principio di necessità nel trattamento dei dati

Contiene un precetto[4] destinato a comportare importanti conseguenze nell'ambito dei trattamenti di dati svolti con sistemi automatizzati. Esso dispone che i sistemi informativi e i software siano configurati in modo da minimizzare il ricorso a dati personali e identificativi, sostituendone il trattamento con l'utilizzo di dati anonimi o pseudonimi quando le rispettive finalità non ne risentano, prevedendo l'identificazione dell'interessato solo in caso di necessità.

Ciò rappresenta una vera rivoluzione nell'approccio alla protezione dei dati trattati con sistemi automatizzati, soprattutto nella sua applicazione al commercio elettronico e al funzionamento dei servizi di telecomunicazione.

[4] Da rilevare che questo principio non è presente né nella Direttiva n. 95/46 né nella legge n. 675/96 ed impone un obbligo alquanto oneroso. Come è possibile, infatti, stabilire se le finalità di un programma possono essere realizzate mediante dati anonimi? Tanto più che la ampiezza della definizione di dato personale rende problematico pensare ad un trattamento che non utilizzi dati personali. Ogni volta che si effettui un trattamento di dati relativi ad un soggetto, anche se durante l'elaborazione avvenga solo su dati apparentemente anonimi tali dati non possono che essere qualificati come personali in quanto, direttamente o indirettamente, relativi ad un certo soggetto.

Art. 4 Definizioni[5]

Risulta ritoccato il ricco apparato di definizioni della legge-base. Non soltanto si è infatti data autonoma considerazione dell'operazione di "consultazione", ma a quelle già previste si sono infatti aggiunte le nozioni di "dati identificativi" e di "incaricati", la formalizzazione delle nozioni di "dati sensibili" e "dati giudiziari", nonché la semplificazione della definizione di "banca dati".

Sono state infine introdotte anche le definizioni traenti origine dalla direttiva n. 2002/58/CE, nonché dalle norme in materia di misure di sicurezza e di trattamento per fini storici, scientifici e statistici[6]. "Titolare", la differenza sostanziale è legata alla formalizzazione dell'esistenza del contitolare del trattamento, figura giuridica che era stata creata dal garante, ma mancava di fondamento legislativo. Il titolare è anche responsabile degli strumenti utilizzati, eliminando possibili dubbi circa gli strumenti di trattamento che compete al titolare.

"Incaricati"[7], sono chiaramente individuati e viene chiaramente detto che l'incaricato può essere solo una persona fisica.

Di particolare importanza in quanto costituiscono una novità rispetto alla legge 675/96 sono:

"dati identificativi", cioè quelli che permettono l'identificazione diretta dell'interessato;

"dati giudiziari", sono i dati personali idonei a rivelare:

* i provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti;
* la qualità di imputato o di indagato.

Art. 5 Oggetto ed ambito di applicazione

Il legislatore delegato ha ripristinato, quale criterio principale di collegamento della fattispecie alla legge applicabile, lo stabilimento nel territorio dello Stato – o in un luogo soggetto alla sua sovranità – del soggetto che effettua il trattamento di dati, ancorché gli stessi siano detenuti all'estero[8]. Nel caso in cui il soggetto che effettua il trattamento sia stabilito in un altro Paese dell'Unione Europea, troverà invece applicazione la legge del Paese di stabilimento.

Quanto all'ipotesi nella quale il soggetto che procede al trattamento sia stabilito in un Paese non appartenente all'Unione Europea, il codice italiano sarà applicabile qualora vengano impiegati, per il trattamento strumenti situati nel territorio dello Stato anche diversi da quelli elettronici (salvo che si tratti di mero transito nel territorio UE). In tale caso il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina in questione.

---

[6] Con l'attuale Codice il nostro Paese ha attuato sostanzialmente la direttiva 12 luglio 2002 n. 2002/58 sul trattamento dei dati nel settore delle telecomunicazioni.

[7] evidente che i responsabili e, soprattutto, gli incaricati possono cambiare con maggior frequenza rispetto ai titolari.

[8] E' irrilevante che i dati personali siano memorizzati ed elaborati su un calcolatore fisicamente dislocato all'estero: se il titolare del trattamento è una società italiana, ad essi si applicherà la legge italiana.

Riguardo al trattamento dei dati personali effettuato da persona fisica, per fini esclusivamente personali, restano applicabili le norme in tema di misure di sicurezza, nonché di risarcimento del danno eventualmente procurato.

Art. 6 Disciplina del trattamento

Le disposizioni contenute nella parte generale (articoli da 1 a 45) si applicano a tutti i trattamenti, ferme le differenziazioni relative al carattere pubblico o privato del soggetto trattante, salvo ove sia espressamente derogata da disposizioni di parte speciale. Le stesse disposizioni di parte speciale potranno, invece, integrare e rendere più specifici e stringenti i precetti di parte generale.

Tale disposizione guida il lettore e lo avverte che i principi applicabili sono tutti nella Parte I, a meno che nella parte successiva trovi esplicite integrazioni o eccezioni nel settore che lo interessa.

TITOLO II
DIRITTI DELL'INTERESSATO

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

I diritti dell'Interessato sono contenuti nel Titolo II.

L'interessato ha diritto di ottenere una serie di informazioni (dalla conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non registrati, all'origine dei dati personali, dall'indicazione delle finalità e modalità del trattamento a quella degli estremi identificativi del titolare, dei responsabili e del rappresentante designato, ecc.) e la modificazione dello stato di cose esistenti, utilizzando lo strumento dell'interpello preventivo, ex art. 146.

L'interessato può opporsi – anche ove non ricorrano motivi legittimi – 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.

Mentre l'art. 13 della L.n. 675/96 qualificava come " gratuito " l'esercizio del corrispondente diritto di opposizione, nel codice attuale non vi è più lo stesso grado di certezza sul carattere gratuito del diritto in parola.

L'art. 7, comma 4, lettera b) non circoscrive più il campo di esplicazione del diritto di opporsi al trattamento di dati personali che lo riguardano a fini, oltre che di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato, anche di comunicazione commerciale tout court, e non già solamente di comunicazione commerciale "interattiva".

<u>L'interessato ha diritto di ottenere:</u>

- la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e l'origine dei dati personali;
- l'indicazione delle finalità e modalità del trattamento;
- gli estremi identificativi del titolare, dei responsabili e del rappresentante designato;
- l'aggiornamento e l'integrazione dei dati;

- la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge[9].

L'interessato ha diritto di opporsi:

- per motivi legittimi al trattamento dei dati personali che lo riguardano;
- al trattamento di dati che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato.

La legge attribuisce agli interessati una posizione di diritto soggettivo, non comprimibile da parte della P.A., in quanto attiene a beni di primaria importanza costituzionale[10].

Art. 8 Esercizio dei diritti

Il codice della privacy consente l'esercizio dei diritti di cui all'art. 7, anche con riferimento a dati personali di carattere non oggettivo. Però l'amplissima gamma delle ipotesi in cui la sua applicabilità è ex lege esclusa - vedi art. 8, comma 2, - rende probabile una rara e comunque controversa sua applicabilità.

In merito al problema dell'accesso da parte del lavoratore o dell'assicurato ai dati contenuti nella cartella personale o nella perizia medica, si distinguono due ipotesi: nel primo caso di solito è in gioco lo sviluppo della carriera o la determinazione della retribuzione; nel secondo caso si tratta quasi sempre di istanze che hanno come base una richiesta di risarcimento.

L'esercizio del diritto di accesso alle banche dati che contengono informazioni personali può avere luogo anche nei confronti dei dati di carattere non oggettivo, "salvo che – l'esercizio del diritto di accesso – concerna la rettificazione o la integrazione dei dati personali di tipo valutativo, relativi a giudizi, opinioni od altri apprezzamenti di tipo soggettivo" e salvo che riguardi " l'indicazione di condotte da tenersi o di decisioni da assumersi da parte del titolare del trattamento"[11]

E' meglio precisata la nozione di "dato personale" che è considerato tale, e quindi pertinente al destinatario oggetto del giudizio e della valutazione, solo quando ha le caratteristiche della conclusività e della definitività, escludendo la qualifica di dato personale al giudizio finalizzato all'indicazione di una condotta dell'impresa o dell'assicurazione. In

[9] Resta il dubbio di sapere chi abbia il potere di determinare quando i dati siano stati trattati "in violazione di legge" e quindi di ordinare la cancellazione o la trasformazione in forma anonima o il blocco. Pare ovvio che nessuna delle parti possa farlo proprio in quanto parti in causa in una eventuale disputa. Si ritiene che solo il Garante o l'Autorità Giudiziaria possa ordinare la cancellazione, trasformazione in forma anonima o il blocco.

[10] La procedura per l'esercizio dei diritti in esame, art. 145 del Codice, prevede il ricorso al Garante con possibilità di impugnazione del suo provvedimento innanzi all'Autorità Giudiziaria Ordinaria o, in alternativa, il ricorso diretto a quest'ultima. La competenza del giudice ordinario è esclusiva.

[11] Il Legislatore ha inteso dire che, mentre non è posto in discussione il diritto di accesso a tutti i dati personali di carattere oggettivo, ossia i dati consolidati e definiti che costituiscono la base della valutazione, viene invece stabilito che quest'ultima non può essere integrata o rettificata ad opera dell'interessato. Viene, inoltre, escluso il diritto di accesso nei confronti dei giudizi, delle opinioni e delle valutazioni che non incidono direttamente sul lavoratore o sull'assicurato, in quanto sono solo preliminari alle decisioni che debbono essere prese dall'azienda. L'interessato può, dunque, chiedere di accedere soltanto all'atto finale assunto dal datore di lavoro o dalla società di assicurazione.

quest'ultimo caso quel giudizio va considerato oggetto di tutela della riservatezza di chi ha effettuato la valutazione.

Art. 9 Modalità di esercizio

Disciplina le modalità relative all' esercizio ed attuazione di siffatti diritti[12]. Tale articolo si ispira a quella logica di semplificazione e di snellimento procedimentale nell'interesse del cittadino che informa l'intero codice della privacy.

Per esercitare il diritto d'accesso è sufficiente inoltrare una richiesta al titolare o al responsabile del trattamento. La richiesta può essere trasmessa con lettera raccomandata, via fax o mediante posta elettronica. Se la richiesta ha come oggetto solo la conoscenza dello stato dei dati (senza alcun intervento su di essi), può essere fatta anche a voce. In tal caso la richiesta viene annotata sinteticamente dal responsabile o dall'incaricato del trattamento.

Il diritto di accesso può essere esercitato anche per delega. La delega o procura deve essere conferita per iscritto dall'interessato e può essere rivolta a persone fisiche, enti, associazioni o organismi.

Art. 10 Riscontro all'interessato

Il Titolare deve dare riscontro alla richiesta e adottare idonee misure organizzative che agevolino e rendano più rapido l'accesso ai dati da parte dell'interessato, secondo una logica di selezione e filtraggio delle informazioni disponibili su un medesimo soggetto, sempre chè la richiesta abbia carattere specifico. Quando l'estrazione dei dati risulti particolarmente difficoltosa, il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali.

Alla luce dell'art. 146, il termine per rispondere alle richieste di accesso diventa più ampio dei 5 giorni previsti dalla L.n. 675/96 passando a 15 giorni e potrà essere ulteriormente allungato se si considera che qualora la richiesta non venisse fatta di persona il Titolare dovrà procedere alla identificazione del soggetto che effettua la richiesta.

In precedenza era previsto un importo massimo da corrispondere quando il titolare non aveva alcun dato del richiedente. La situazione adesso è cambiata in quanto è prevista la possibilità che il titolare richieda un compenso, almeno parziale, per le spese sostenute per le ricerche richieste dall'interessato, soprattutto quando il titolare è obbligato a fotocopiare grandi quantità di documenti. Si pensi ad esempio alla richiesta di una copia di una radiografia per la quale in precedenza il garante aveva stabilito che era sufficiente, per il titolare, consegnare il referto radiologico, anziché la radiografia vera e propria.

Con questa nuova disposizione, l'interessato può anche chiedere una copia della radiografia, a condizione di pagarne i costi.

TITOLO III
REGOLE GENERALI PER IL TRATTAMENTO DEI DATI
Capo I

[12] Mentre l'art. 13 della L.n.675/96 stabiliva che l'interessato aveva diritto di ottenere certe informazioni da parte del titolare, il nuovo art. 7 non attribuisce quest'obbligo al titolare ma da una lettura combinata degli artt. 7/10 se ne deduce che l'obbligo spetta nel complesso al Titolare, che però può delegarlo ad un responsabile designato.

Regole per tutti i trattamenti

Art. 11 Modalità del trattamento e requisiti dei dati

E' rinvenibile un sostanziale adeguamento ai principi comunitari in materia di raccolta e trattamento dei dati posto che per le modalità di trattamento si richiede che i dati personali siano trattati in modo lecito e secondo correttezza, siano raccolti per finalità esplicite[13], legittime e determinate, e che il trattamento non ecceda le finalità per le quali i dati sono raccolti o successivamente trattati e che sia temporalmente limitato[14].

Il comma 2 dell'articolo sancisce la non utilizzabilità dei dati che siano stati trattati in maniera difforme dalla disciplina rilevante. La non utilizzabilità dei dati è una novità introdotta dal Codice e sembra essere differente da altre ipotesi di blocco o divieto dei trattamenti, previsti dagli artt. 143 e 154.

Art. 12 Codici di deontologia e di buona condotta

Il legislatore ha previsto una speciale procedura di formazione del codice che, mediante la verifica di conformità ai principi generali della legge operata dal Garante, riconosce ai codici deontologici il valore di criterio di riferimento per determinare la legittimità del trattamento. Il rispetto delle regole contenute nei codici costituisce elemento certo per la valutazione, anche nell'eventuale sede giudiziaria, del rispetto dei principi di lealtà e correttezza del trattamento. Il codice deontologico, assume, quindi, valenza di norma, sebbene di grado secondario rispetto alla legge[15].

Per diversi settori di attività, il Codice impone l'adozione di appositi codici deontologici, il cui rispetto rappresenta una condizione essenziale per la liceità dei trattamenti medesimi ed i dati trattati in violazione della normativa non possono essere utilizzati[16].

Art. 13 Informativa

Il trattamento dei dati personali passa attraverso l'informativa che consiste in una dichiarazione che il Titolare e/o il Responsabile fa all'interessato, in forma scritta od orale,

---

[13] Il principio della finalizzazione è, in buona sostanza, un principio di trasparenza: per effettuare un trattamento di dati, occorre che esso sia stato dichiarato e ne siano state definite le finalità.

[14] E' fatta salva l'applicazione di particolari cautele – rimesse al prudente e tecnico apprezzamento del Garante – per i trattamenti che presentano rischi specifici.

[15] L'effettivo rispetto dei menzionati principi è assicurato dai vari Codici di autodisciplina promossi dal Garante tra le categorie interessate, alle cui prescrizioni devono conformarsi i titolari del trattamento perché le operazioni dagli stessi poste in essere possano dirsi legittime e corrette. Tali Codici dovranno, previa approvazione del Garante, essere pubblicati sulla G.U. e costituiranno quindi la normativa secondaria ed applicativa dello stesso codice.

[16] Al momento i codici deontologici pubblicati e riportati nell'Allegato A) sono: 1. l'attività giornalistica; 2. il trattamento dei dati per scopi storici; 3. il trattamento dei dati a scopi statistici e di ricerca, effettuato nell'ambito del sistema statistico nazionale. A seguire si aggiungeranno altro codici tra cui quello relativo ai trattamenti di dati personali effettuati con strumenti automatizzati di rilevazione di immagini, che di recente è stato adottato.

delle maggiori caratteristiche relative all'utilizzo delle informazioni che lo riguardano. L'informativa è uno strumento che indica il percorso che i dati seguiranno ed è per questo che deve essere chiara, essenziale e veritiera, per consentire all'interessato di "andarsi a riprendere" i dati o di verificare, in qualunque momento, se il trattamento avviene nel rispetto delle regole previste.

Il contenuto dell'Informativa è previsto espressamente dal Legislatore; essa serve, quindi, per consentire all'interessato l'esercizio e il controllo diretto sulle operazioni di trattamento sui propri dati personali. L'interessato è consapevole dell'ambito di circolazione delle informazioni che lo riguardano e può riappropriarsene, esercitando quel diritto all'autodeterminazione informativa che è a fondamento della disciplina stessa.

A differenza di quanto stabilito dalla L. 675/96 che non prevedeva che dovessero essere inclusi nella informativa i nominativi dei responsabili e degli incaricati, che potrebbero venire a conoscenza *dei* dati, l'attuale codice stabilisce al lettera d) che occorre indicare nella informativa"i soggetti o le categorie di soggetti ai quali i dati personali possono essere omunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati"[17]. Considerata la funzione di trasparenza svolta dalla informativa, questo adempimento risulta obbligatorio, salvo rare eccezioni, in qualsiasi contesto.

Il rilascio della informativa costituisce sia una condizione di validità del consenso successivamente prestato dall'interessato al trattamento dei suoi dati che una condizione essenziale per poter esercitare i diritti di accesso e di opposizione al trattamento dei suoi dati riconosciutigli dall'art. 7 del codice privacy. L'informativa va rilasciata, prima della raccolta dei dati, al soggetto interessato oppure ai soggetti terzi presso i quali siano stati raccolti i dati dell'interessato.

Art. 13, comma 5: Nell'ipotesi di raccolta di dati da fonti diverse dall'interessato non si è tenuti a osservare l'obbligo di rilascio dell'informativa qualora il trattamento costituisca un obbligo di legge o sia finalizzato allo svolgimento di investigazioni difensive oppure l'informativa comporti un impiego di mezzi che il Garante dichiari manifestamente sproporzionato.

Se i dati vengono raccolti presso un elenco pubblico, ad es. albo professionale, l'obbligo della informativa spetta a chi vorrà trattare i dati ad es, per finalità di marketing in quanto tali finalità sono diverse dalle finalità inerenti la pubblicazione in un albo pubblico. Non sarà necessario il consenso, ma il soggetto che raccoglie i dati presso un albo dovrà comunque fornire l'informativa.

L'informativa può essere data oralmente o per iscritto. Il rilascio dell'informativa per iscritto consente di precostituire la prova dell'avvenuta esecuzione dell'adempimento.

Il Legislatore ha previsto modalità semplificate per il rilascio dell'informativa, come nel caso di trattamenti per finalità sanitarie.

L'omissione dell'informativa[18] è punita con la sanzione amministrativa del pagamento di una somma il cui importo aumenta se si tratta di dati sensibili o giudiziari o che presentano rischi specifici ex art. 17.

---

[17] Questa nuova stipulazione rende estremamente complessa la informativa e soprattutto la assoggetta ad un continuo aggiornamento, perché è evidente che i responsabili e, soprattutto, gli incaricati possono cambiare con maggior frequenza rispetto ai titolari. Si può ritenere che i soggetti, responsabile e incaricati, non dovranno però essere indicati nominalmente ma andranno individuati a livello di tipologia di soggetti.

[18] Si manda all'art. 161 del Codice, per quanto attiene alle sanzioni che scattano in caso di omessa o inidonea informativa.

Art. 14 Definizione dei profili e della personalità dell'interessato

Il Legislatore ha disciplinato l'utilizzo dei profili elettronici [19] – da intendere come quelle situazioni in cui si delega, in via esclusiva, allo strumento elettronico una valutazione relativa al comportamento umano – quando il procedimento di valutazione è affidato in via esclusiva alla macchina, senza l'assistenza dell'uomo.

Se, invece, la valutazione è frutto di un procedimento composito, caratterizzato dall'interazione di un operatore con uno strumento elettronico che funge da supporto alla di lui valutazione soggettiva allora la procedura non è sanzionata.

Art. 15 Danni cagionati per effetto del trattamento[20]

Tale articolo prevede che "chiunque cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'art. 2050 c.c.", con la conseguenza che l'autore del danno deve dimostrare di avere adottato tutte le misure idonee a evitare il danno. E' noto che qualora un'attività o una cosa produca danno non per la sua intrinseca natura o per l'insorgenza in essa di agenti dannosi, ma perché inserita in un'attività pericolosa, trova applicazione la presunzione di responsabilità prevista dall'art. 2050 del c.c.

Il trattamento dei dati personali è considerato quindi dal Legislatore attività pericolosa. La Cassazione con sentenza n. 3022 del 2001 ha stabilito che " si intendono per attività pericolose, in relazione al cui svolgimento opera la presunzione, oltre quelle prese in considerazione per la prevenzione degli infortuni e la tutela dell'incolumità pubblica, tutte quelle altre che, pur non essendo specificate o disciplinate, presentino una pericolosità intrinseca o dipendente dalle modalità di esercizio e dai mezzi adoperati".

Pertanto, chi ritenga di essere stato leso a seguito dell'attività di trattamento dei dati personali che lo riguardano può ottenere il risarcimento dei danni senza dovere provare la colpa del Titolare che ha trattato i suoi dati. L'interessato deve però provare[21] eventuali danni derivanti dal trattamento dei dati. L'interessato dovrà provare il nesso di causalità [22], quindi che:

a) il danno[23] si sia realizzato[24], e

---

[19] Il tema della **profilazione dell'utente** attiene alla ricostruzione dei suoi gusti e delle sua abitudini attraverso l'archiviazione dei suoi dati. Il Codice vieta ad ogni Autorità, giudiziaria o amministrativa, di emettere un atto o un provvedimento che implichi una valutazione del comportamento umano fondato "unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato".

[20] La **responsabilità civile** è disciplinata da disposizioni collocate in diversi articolo del Codice. Norma fondamentale è però l'art. in questione il quale va incrociato con le disposizioni di cui all'art. 152, commi 1 e 15, in base alle quali: a. sussiste la giurisdizione esclusiva dell'Autorità Giudiziaria Ordinaria in merito ad ogni controversia riguardante l'applicazione della legge stessa; b. la violazione delle regole poste dall'art. 11 per la raccolta dei dati comporta il risarcimento anche del danno non patrimoniale (art. 15, comma 2), cioè del **danno morale** consistente nella sofferenza patita dal proprietario dei dati per essere stati gli stessi trattati in modo non conforme alle disposizioni normative. L'Autorità giudiziaria dovrà quindi liquidare, tra le voci di danno, il pretium doloris.

[21] **La struttura dell'illecito.** I diversi elementi che compongono l'illecito sono: il **fatto** (azione od omissione), la **riferibilità del fatto alla P.A.,** l'**evento dannoso,** il **nesso di causalità e** l'**elemento soggettivo.**

[22] Il **nesso di causalità** è disciplinato dalle regole ordinarie.

[23] Il **fatto** può consistere in una qualunque delle operazioni di trattamento, di cui all'art. 4 del Codice, ma può perfezionarsi anche con l'omissione di un adempimento dovuto: rileva la

b) dipenda dall'attività di trattamento [25].

Colui che ha effettuato il trattamento, per sottrarsi all'obbligo di risarcimento, ha l'onere di provare di avere adottato tutte le misure idonee a evitare il danno, secondo il principio dell'inversione dell'onere della prova[26].

La domanda di risarcimento dei danni va avanzata dal soggetto interessato nei confronti del Titolare.

---

mancata adozione delle misure di sicurezza prescritte. Il verificarsi di un danno conseguente alla mancata adozione delle misure di sicurezza obbligatorie comporterà la responsabilità dell'agente. Se la natura particolare dei dati o delle operazioni che su di essi devono essere svolte, o di altre circostanze lo richiedano, la P.A. dovrà adottare anche misure ulteriori richieste dalla situazione concreta per "evitare il danno", altrimenti la prova liberatoria non potrà essere fornita.

[24] L' **evento dannoso** consiste nella perdita di informazioni personali, che si qualifica nel senso di "danno ingiusto" laddove detta perdita avvenga a seguito della violazione di una delle disposizioni poste dal Codice per lo svolgimento dei trattamenti dei dati personali. Per quanto attiene ai **dati comuni,** l'antigiuridicità dell'evento andrà valutata in relazione alla connessione delle operazioni di trattamento con lo svolgimento di funzioni istituzionali da parte del soggetto attivo: il trattamento si qualificherà in senso antigiuridico laddove avvenga per motivi non attinenti al raggiungimento degli obiettivi di pubblico interesse che le leggi, i regolamenti, ed in generale gli atti del potere politico assegnano all'Ente. Per quanto riguarda, invece, i **dati sensibili o giudiziari,** costituisce evento dannoso antigiuridico la perdita dei dati personali correlata a trattamenti che l'Amministrazione abbia posto in essere fuori dai casi previsti da "espresse disposizioni di legge", o effettuati senza rispettare le modalità e le limitazioni da queste prescritte, o le norme generali ex art. 22 per il trattamento dei dati sensibili e giudiziari da parte della P.A. Costituirà **danno ingiusto** la perdita di dati correlata a trattamenti che la P.A. abbia posto in essere senza avere emanato il suddetto regolamento o incidendo su dati personali esclusi da questo o ancora effettuando operazioni che esso non autorizza.

[25] La **riferibilità del fatto all'Amministrazione** sussiste in tanto in quanto essa possa ritenersi esplicazione di una delle funzioni istituzionali della stessa. Laddove il fatto avvenga per uno scopo ch efuoriesce dall'attività propria dell'Amministrazione o addirittura collide con esso, l'agente sarà l'unico soggetto tenuto al risarcimento. Il risarcimento potrà essere richiesto, in via alternativa, al dipendente dell'Amministrazione o a quest'ultima. Nel caso in cui l'Amministrazione sia costretta a pagare il prezzo del risarcimento dei danni provocati da propri dipendenti potrà effettuare la rivalsa nei loro confronti; a tal fine sarà necessario incardinare il processo per la responsabilità amministrativa innanzi alla Corte dei Conti, al termine del quale il dipendente, autore del danno, dovrà rimborsare all'Amministrazione ciò che questa ha risarcito, ma solo se il primo ha agito con dolo o colpa grave. Non configura necessariamente un caso di colpa grave la mancata adozione di misure di sicurezza ulteriori, non previste nei regolamenti ma comunque indispensabili nel caso concreto. Non dovrebbe configurare un caso di colpa grave neanche il fatto di procedere alla ostensione di documenti amministrativi contenenti dati personali di terzi a fronte di una richiesta di accesso.

[26] l' **elemento soggettivo.** Ai sensi dell'art. 2043 del c.c., l'illecito civile può essere punito solo se l'autore del fatto abbia agito con dolo, cioè con l'intento di cagionare un danno ingiusto alla vittima, o con colpa, cioè violando regole (comuni o specifiche) di prudenza, diligenza e perizia. Per alcuni, la **prova liberatoria** richiesta dall'art. 2050 del c.c. attiene alla diligenza professionale: l'autore del danno deve cioè provare di avere adottato le misure di prudenza e di diligenza che sono appropriate a quelle particolari operazioni di trattamento

L'area dei danni risarcibili per la violazione del diritto alla riservatezza è estesa anche al danno non patrimoniale, nel caso in cui il Titolare violi i principi generali sulla privacy indicati all'art. 11, la quantificazione del danno non patrimoniale si basa su una valutazione di equità, ai sensi degli articoli 1226 e 2056 del c.c.

Art. 16 Cessazione del trattamento

In caso di cessazione del trattamento di dati personali, l'Ente potrà solo: 1. distruggerli; 2. cederli a terzi che, a loro volta, potranno utilizzarli unicamente per trattamenti finalizzati agli stessi scopi di quello cessato; 3. conservarli per fini esclusivamente personali; 4. conservarli o cederli ad altro titolare, per scopi di ricerca storica, scientifica o statistica. La cessione del trattamento non si verifica nell'ipotesi di cessione dell'Azienda o di un ramo di essa ma solo quando "il trattamento venga a cessare oggettivamente od il titolare intenda porvi fine".

La cessione illegittima comporta l'irrogazione della sanzione amministrativa del pagamento di una somma. (art. 162, comma 2).

Art. 17 Trattamento che presenta rischi specifici

E' in assoluto la norma più indeterminata nel contenuto e oscura nelle sua determinazioni! Trattasi di una fattispecie introdotta in Italia dal d.Lgs.vo n. 467/2001.

Si tratta di tipologie di dati[27] non sensibili né giudiziari, che si differenziano dai dati comuni a causa della loro potenzialità lesiva per i diritti, le libertà fondamentali o la dignità dei titolari. Questa categoria non è identificata in concreto: è il Garante che ad ogni inizio di trattamento che gli sia notificato dovrà valutare se questo, per la natura dei dati elaborati, le conseguenze che può provocare o le modalità con cui si svolgerà, presenti la suddetta pericolosità. Le disposizioni in materia di dati particolari si applicano sia ai soggetti privati che alle P.A.

La mancata adozione delle misure previste dal Garante costituisce un reato punito allo stesso modo della violazione delle norme sul trattamento dei dati sensibili. (art. 167, comma 2).

Capo II
Regole ulteriori per i soggetti pubblici[28]

[27] Rientrano in questa categoria di dati le c.d. informazioni reddituali, qualificate come "dati particolari" dal D.lgs.vo n. 135/98. Tali dati potranno essere oggetto di specifica prescrizione da parte del Garante.

[28] Il Codice fissa i principi in base ai quali un soggetto pubblico è legittimato a trattare i dati personali. La disciplina è differenziata in funzione della natura dei dati personali. Le condizioni e i limiti posti all'azione della P.A. crescono al crescere dei rischi per la riservatezza dell'individuo. Per questa ragione il Codice identifica: 1. principi applicabili a tutti i trattamenti, indipendentemente dalla natura dei dati. Essi riguardano sia i dati comuni sia i dati sensibili o giudiziari; tale fattispecie è disciplinata nell'art. 18; 2. principi applicabili al trattamento dei c.d. dati comuni (art. 19); 3. principi applicabili al trattamento dei dati definiti sensibili; (art. 20); 4. principi applicabili al trattamento dei dati definiti giudiziari (art. 21); 5. principi applicabili al trattamento dei dati sensibili e giudiziari (art. 22).

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

Il codice chiarisce che i soggetti pubblici – salve le disposizioni riguardanti medici e organismi sanitari – non debbono richiedere il consenso dell'interessato: esso non solo non costituisce un requisito del trattamento, ma non va neppure richiesto o sollecitato dalle amministrazioni pubbliche[29].
La raccolta e il trattamento dei dati, diversi da quelli sensibili o giudiziari, (eccettuate la comunicazione e la diffusione) sono infatti consentiti ai soggetti pubblici parallelamente allo svolgimento delle funzioni istituzionali, anche in mancanza di norme di legge o di regolamento che li prevedano espressamente.
La fonte di legittimazione al trattamento è l'attività pubblicistica svolta dall'Ente e in questo concetto rientrano tutti i suoi compiti, propri e delegati[30]. Il concetto di "funzioni istituzionali" va inteso, quindi, in senso ampio come attività rivolte al perseguimento degli interessi collettivi, e può trovare fondamento, oltre che nella legge anche in atti di indirizzo emanati dagli organi di governo dell'Ente, a condizione che si tratti di atti assunti legittimamente[31].
Nel bilanciamento tra l'interesse alla tutela del diritto alla riservatezza che il singolo vanta sulle informazioni che lo riguardano, e l'interesse all'efficacia e speditezza nel perseguimento degli interessi collettivi da parte delle P.A., la legge assegna quindi maggiore rilievo al secondo elemento[32].
Il trattamento illegittimo di dati personali da parte di dipendenti delle P.A. costituisce reato punibile con la reclusione fino a 18 mesi. E' un reato a dolo specifico, perché la sua consumazione richiede non solo l'assenza di presupposti legittimanti il trattamento, ma anche lo scopo di ottenere un profitto o di arrecare un danno a terzi. Per la punibilità del fatto è indispensabile che un danno si verifichi.
.

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

[29] L'esenzione della P.A. dall'obbligo di acquisizione del consenso costituisce una semplificazione rispetto a quanto richiesto ai privati e agli e.p. economici, i quali, invece, devono basare la loro attività, come regola generale, sul consenso dell'interessato.
[30] Il principio di finalità previsto dal comma 2 dell'art.18, rappresenta l'elemento centrale del sistema che differenzia i due settori pubblico e privato. Tale principio consiste nel dovere, da parte del soggetto pubblico, di utilizzare i dati personali esclusivamente per lo svolgimento delle funzioni istituzionali. Sono funzioni istituzionali, sia i trattamenti "indispensabili per la realizzazione delle attribuzioni dell'ente" si quelli "volti comunque ad agevolare o rendere più rapida la realizzazione degli interessi pubblici affidati al soggetto".
[31] Resta da vedere se il discorso fin qui svolto, in merito alla legittimazione delle P.A. al trattamento di dati personali, valga anche per la c.d. "attività privata di diritto privato" degli Enti Pubblici, o se invece questa resti esclusa dal campo di applicazione dell'art. 18, con conseguente necessità del consenso dell'interessato al trattamento
[32] Il secondo principio che costituisce una ulteriore condizione limitativa dell'attività della P.A. è rappresentato dal principio di legalità, di cui al 3° comma dell'art.18. Tale principio consiste nel dovere, da parte del soggetto pubblico, di eseguire le operazioni di trattamento osservando anche i limiti fissati dalle leggi e dai regolamenti dello specifico settore di attività.

I soggetti pubblici, esclusi gli enti pubblici economici, possono trattare i dati personali comuni solo per lo svolgimento delle proprie finalità istituzionali e, a tale fine – a parte quanto espressamente previsto in ambito sanitario – gli stessi non devono chiedere il consenso degli interessati[33].
Perché però i dati trattati da un'amministrazione possano essere conosciuti al di fuori di essa, non è sufficiente fare riferimento alle funzioni istituzionali, ma occorre che un'apposita norma di legge o di regolamento ne preveda la comunicazione o la diffusione (fanno eccezione i casi di comunicazione fra soggetti pubblici, per i quali può risultare sufficiente informare preventivamente il Garante).
La comunicazione di dati da soggetto pubblico a soggetto pubblico è consentita: 1. come regola generale, quando è prevista espressamente da una norma di legge o di regolamento,; o 2. in mancanza di una specifica norma di legge o di regolamento sulla base di una autorizzazione del Garante. (art. 19, comma 2)
La comunicazione di dati comuni da soggetto pubblico a soggetto privato può avvenire in due ipotesi se: 1. la comunicazione di dati comuni a uno o più soggetti privati inclusi gli e.p. economici; o 2. la diffusione di dati comuni a soggetti indeterminati. Tali operazioni sono consentite unicamente quando risultano previste da una norma di legge o di regolamento (principio di legalità). In assenza di ciò tali operazioni risultano inibite.

Art. 20 Principi applicabili al trattamento di dati sensibili

Tale articolo stabilisce che il trattamento dei dati sensibili da parte dei soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati: a) le finalità di rilevante interesse pubblico perseguite; b) le operazioni che possono, con quei dati, essere effettuate e c) i tipi di dati che possono essere utilizzati.
Nel caso che una legge del genere non esista, l'Ente interessato, per potere procedere al trattamento, deve chiedere al Garante di dichiarare la sussistenza di un interesse pubblico rilevante connesso agli scopi del trattamento in questione[34]. Nei casi in cui la norma di legge specifica tali scopi ma non i tipi di dati e le operazioni eseguibili allora questi ultimi dovranno essere identificati e resi pubblici dalle singole Amministrazioni con regolamenti. Per i trattamenti già in atto i regolamenti devono essere emanati entro il 30 settembre 2004, (ex art. 181, comma 1, lett. A.)
Il Codice prevede una tutela rafforzata anche per le informazioni sui precedenti penali di un soggetto desumibili dal casellario giudiziale. Tali dati giudiziari possono essere trattati solo su autorizzazione: contenuta espressamente in una norma di legge o contenuta in un provvedimento del Garante. Sia la prima che il secondo legittimano il trattamento dei dati giudiziari in quanto specifichino gli scopi di pubblico interesse connessi al trattamento, le tipologie di dati oggetto di questo e le operazioni che possono essere eseguite; in caso

[33] Al soggetto pubblico è consentito effettuare un trattamento di dati comuni, diverso da comunicazione o diffusione, anche in assenza di una norma di legge o di regolamento che lo prevede in modo esplicito.
[34] Mentre ai sensi del comma 2 dell'art. 20 se esiste una legge che disciplina le rilevanti finalità di interesse pubblico perseguite ma non indica espressamente i titpi di dati sensibili che possono essere trattati e le operazioni che possono essere eseguite, allora si sopperisce alla lacuna di legge attraverso un regolamento interno dell'ente; nella fattispecie di cui al comma 3 – quando cioè manchi una espressa disposizione di legge riguardo ai dati sensibili – il trattamento deve essere autorizzato dal Garante.

contrario le Amministrazioni dovranno chiedere l'autorizzazione al Garante o emanare appositi regolamenti.

Art. 21 Principi applicabili al trattamento di dati giudiziari[35]

Il trattamento è consentito qualora:
1. risulti autorizzato da una disposizione di legge che indichi in modo espresso:
1. le finalità perseguite che devono essere riconosciute e dichiarate esplicitamente di valore "rilevante"; i tipi di dati giudiziari che possono essere trattati; i tipi di operazioni che possono essere eseguite; oppure,
2. risulti autorizzato da un provvedimento del Garante che indichi in modo espresso: le finalità perseguite; i tipi di dati giudiziari che possono essere trattati, e i tipi di operazioni che possono essere eseguite[36].
In base alla fattispecie regolata dal comma 2, se esiste una legge che specifica espressamente la finalità di rilevante interesse pubblico perseguito ma non indica espressamente i tipi di dati giudiziari che possono essere trattati e i tipi di operazioni eseguibili, allo è necessario adottare un regolamento interno che circoscriva l'attività del soggetto pubblico.

Art. 22 Principi applicabili al trattamento di dati sensibili e giudiziari

In riferimento al trattamento dei dati sensibili e giudiziari, i soggetti pubblici possono trattare tale categoria di dati quando ciò rientra nel novero delle rilevanti finalità di interesse pubblico stabilite per legge o attraverso un provvedimento del Garante. Il tutto previa identificazione delle operazioni eseguibili e delle tipologie di dati impiegabili per via regolamentare.
Per tali categorie di dati l'informativa deve contenere anche l'indicazione della norma (statale o regionale) che prevede lo svolgimento dei compiti per i quali è necessario il trattamento.
Per la corretta gestione dei dati sensibili e giudiziari da parte della P.A. occorre che:

- i dati[37] devono essere trattati solo nei casi strettamente necessari per l'espletamento delle attività istituzionali e solo quando non sia possibile utilizzare dati comuni od anonimi[38];
- le P.A. devono verificare periodicamente che i dati sensibili raccolti siano esatti[39];

[35] Il Codice definisce come giudiziari i dati idonei a rivelare i provvedimenti 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 artt. 60 e 61 del c.p.p.
[36] Tutti gli elementi citati devono risultare desumibili dal testo di legge o dal provvedimento del garante; non è ammessa alcuna interpretazione induttiva ed estensiva.
[37] Art. 22, comma 1, Tutela dei diritti individuali. Deve essere valutata, preventivamente e caso per caso, quale sia la scelta più appropriata in relazione alle modalità di raccolta e utilizzo dei dati sensibili e giudiziari allo scopo di garantire che il soggetto non abbia a soffrire della violazione dei suoi diritti, delle libertà fondamentali e della sua dignità.
[38] Art. 22, commi 3 e 9, Principio di indispensabilità sancisce che il ricorso all'uso di dati sensibili o giudiziari anziché di dati anonimi per svolgere una determinata attività deve, per un soggetto pubblico, rivelarsi indispensabile non bastando il principio di necessità valido per i privati.
[39] I dati non indispensabili, eccedenti o non pertinenti non possono essere utilizzati.

- i dati[40] contenuti in elenchi, registri o banche dati gestiti con l'ausilio di sistemi informatici devono essere trattati con tecniche di cifratura o con codici identificativi o altri sistemi che permettono di identificare gli interessati solo in caso di necessità[41].
- i dati idonei a rivelare lo stato di salute e la vita sessuale devono essere archiviati separatamente da ogni altro tipo di dato; ciò a prescindere dalle modalità di trattamento dei dati, cartacea e/o informatizzata.
- è vietato utilizzare dati sensibili o giudiziari per test psicoattitudinali.

La violazione di queste disposizioni costituisce reato punibile con la reclusione. E' un reato a dolo specifico che richiede l'assenza dei presupposti legittimanti il trattamento, lo scopo di ottenere un profitto o di arrecare un danno a terzi. La punibilità del fatto è subordinata alla condizione che si sia verificato un danno.

CAPO III
Regole ulteriori per privati ed enti pubblici economici

Art. 23 Consenso

Il consenso è una libera ed esplicita manifestazione di volontà dell'interessato in relazione all'utilizzo dei propri dati personali da parte di terzi che in qualità di Titolari del trattamento dei dati ne decidono le finalità e le modalità. Il consenso rappresenta, assieme all'esercizio del diritto di accesso e di opposizione al trattamento, il potere dell'interessato di auto determinare il proprio patrimonio informativo.
Il consenso va richiesto all'Interessato, prima della raccolta dei dati, salvo particolari situazioni in cui il Legislatore ammette la possibilità di richiedere e rilasciare il consenso da parte di un soggetto diverso da quello cui si riferiscono le informazioni (come nel caso di incapacità fisica o mentale dell'interessato o del consenso rilasciato da chi esercita la patria potestà, in relazione ai minori).
Il consenso costituisce una condizione di liceità del trattamento dei dati posto in essere da parte dei privati e degli enti pubblici economici.
Il consenso deve essere informato e la informativa costituisce condizione di validità del consenso stesso: non è valido un consenso se non è preceduto da una informativa adeguata.
Il consenso deve essere espresso, non è valido il consenso implicito e può riguardare anche una o più parti delle operazioni di trattamento.
Detto obbligo non sussiste nei casi espressamente previsti dal legislatore (art. 24).
Il 3° comma stabilisce che il consenso per il trattamento dei dati comuni "è documentato per iscritto" ciò vuol dire che non è obbligatoria la espressione del consenso per iscritto ma è sufficiente che l'interessato esprima il suo consenso e che tale espressione sia documentata per iscritto.

[40] L'accesso ai dati deve essere consentito unicamente alle persone autorizzate in possesso di password e user id e l'associazione dato-individuo deve essere consentita solo in caso di necessità operativa.
[41] Anche i dati idonei a rivelare lo stato di salute tenuti con archivi cartacei devono essere oggetto di trattamento con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che li rendono temporaneamente intelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

Se invece il trattamento ha ad oggetto dati sensibili allora il consenso deve essere manifestato in forma scritta. Ciò significa che l'interessato deve fisicamente apporre la propria firma su un modulo di consenso.
In linea generale, per i trattamenti di dati personali effettuati dalla P.A. il consenso dell'interessato non costituisce una condizione di liceità. (art. 18, comma 4) Unica eccezione riguarda l'uso dei dati sulla salute da parte di professionisti sanitari o di organismi sanitari pubblici a fini di tutela della salute.
La forma del consenso. Il consenso deve essere manifestato in forma scritta nel caso in cui il trattamento abbia a oggetto i dati sensibili mentre il legislatore per il legittimo trattamento dei dati comuni richiede che il consenso sia esplicito. Unica eccezione a questa dicotomia " dati sensibili – non sensibili ", riguarda l'uso dei dati sulla salute (= dati sensibili) a fini sanitari, che ammette la formula del consenso verbale documentato per iscritto.
Il legislatore ha previsto ipotesi in cui il consenso può essere rilasciato con modalità semplificate (es. il trattamento di dati sulla salute a fini sanitari).

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

Per alcuni dati sensibili il trattamento può avvenire anche senza consenso, previa autorizzazione del Garante, quando:

a) il trattamento è effettuato da associazioni[42], enti od organismi senza scopo di lucro relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'ente;
b) il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo;
c) il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive o per fare valere in sede giudiziaria un diritto;
d) 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;
e) quando il trattamento abbia ad oggetto dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;
f) quando il trattamento sia necessario, in conformità ai rispettivi codici di deontologia, per esclusivi scopi scientifici o statistici, o per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico.

Manca a tale lista di eccezioni quella con i casi in cui il consenso non sia necessario "per perseguire un legittimo interesse del titolare" "qualora non prevalgano le libertà fondamentali o i diritti dell'interessato"[43]. Questo principio, in forma generale, è presente nella Direttiva che prevede, appunto, che il consenso non sia necessario per perseguire un legittimo interesse del titolare, qualora non prevalgano le libertà fondamentali o i diritti dell'interessato.

Art. 25 Divieti di comunicazione e diffusione

[42] In questa ipotesi però è esclusa la possibilità sia della diffusione sia della comunicazione.
[43] Ad es. nell'ambito di un rapporto di lavoro non dovrebbe essere richiesto il consenso per: la predisposizione degli elenchi telefonici interni, la prenotazione di sale riunioni, la concessione in uso di beni aziendali, quali: pc, autovetture, ecc.

La comunicazione e la diffusione sono vietate sia a seguito di disposizioni adottate dal Garante o dalla autorità giudiziaria anche nei due casi disciplinati dal legislatore:

1. per quei dati personali di cui è stata ordinata la cancellazione;
2. quando la comunicazione e/o la diffusione avvengano per finalità difformi da quelle indicate nell'atto di notificazione.

Art. 26 Garanzie per i dati sensibili[44]

Tale norma permette il trattamento dei dati sensibili solo con il consenso scritto dell'interessato e previa autorizzazione del Garante che può, in ogni tempo, prescrivere quelle misure e quegli accorgimenti ritenuti opportuni a garanzia dell'interessato e che il Titolare del trattamento è tenuto ad adottare.
Si deroga a tale regola del consenso scritto e della previa autorizzazione del Garante per quei 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" e per i "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".
I dati sensibili possono essere oggetto di trattamento anche senza il consenso dell'Interessato, purchè previa autorizzazione del Garante,
1. "quando il trattamento è effettuato da associazioni, enti o organismi senza scopo di lucro…per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto,…";
2."quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo…";
3. "quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive o per fare valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati 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";
4. "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…".

Art. 27 Garanzie per i dati giudiziari

Il legislatore ha previsto anche le garanzie per i dati giudiziari prescrivendo che il loro trattamento " è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni autorizzate".

[44] La definizione di dato sensibile è inserita nella sezione di definizioni dell'art. 4, comma 1, lett. d). Essa suscita le seguenti perplessità: la dizione "dati idonei" introduce, rispetto alla direttiva europea un concetto di potenzialità che allarga a dismisura la categoria di dati sensibili; inoltre, in merito alla dizione relativa alle convinzioni "di altro genere", di quale genere di convinzioni si tratta? La genericità della espressione usata è da sottolineare negativamente in quanto si tratta pur sempre di una norma sanzionata penalmente dall'art. 167 del Codice.

TITOLO IV
SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

Art. 28 Titolare del trattamento

Il codice chiarisce il concetto che titolare è l'entità nel suo complesso, o una qualsiasi unità, anche periferica, alla sola condizione che eserciti un potere autonomo[45].
Il Titolare, pertanto, è il soggetto che esercita un potere decisionale del tutto autonomo sulle finalità e modalità del trattamento, ivi compreso il profilo della sicurezza. Può essere una persona fisica, una persona giuridica o un ente.
La novità è che è titolare dei dati anche chi decide "unitamente ad altro titolare": si sancisce così la validità di ipotesi di con titolarità dei trattamenti.
Il Garante non ha escluso la possibilità di scindere la titolarità dal suo esercizio. Il principio fondamentale in merito alla delega è quello dell'effettività: una delega è efficace, quando il delegato riceve anche i poteri che gli consentono di esercitare in modo effettivo i compiti attribuitigli. Titolare, pertanto, può essere anche l'unità o l'organismo che esercita un potere decisionale autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Art. 29 Responsabile del trattamento

Nessuna modifica significativa sulla definizione di responsabile del trattamento; si chiarisce, però, che è possibile suddividere i compiti tra più responsabili.
Il Responsabile è la persona fisica o giuridica che può essere designata – per iscritto - da parte del titolare del trattamento[46]. Dovrà sempre essere scelto tra persone che per esperienza o capacità forniscano idonea garanzia sul pieno rispetto delle norme in materia di trattamento dei dati, compreso il profilo della sicurezza.
Al quinto comma è ribadito il concetto fondamentale che il responsabile in realtà responsabile non è, in quanto la responsabilità finale sulle sue operazioni compete al titolare, che deve oltretutto vigilare sull'operato del responsabile, anche tramite verifiche periodiche.

Art. 30 Incaricati del trattamento

Viene riconosciuta nuova dignità agli incaricati del trattamento precisando che sono tali coloro che operano sotto la diretta autorità del titolare o del responsabile, nel quadro di istruzioni specifiche.
Incaricato è chiunque compie operazioni di trattamento. Possono essere individuati come incaricati solo le persone fisiche e non anche le persone giuridiche, mentre il requisito che

[45] Ciò non toglie che, ai fini dell'attribuzione di responsabilità varranno nei confronti del titolare le norme in materia di rappresentanza dell'entità titolare. In altre parole, se titolare è l'azienda, chi risponde per eventuali illeciti sarà chi rappresenta l'azienda stessa.
[46] E' prassi comune che nell'ambito di alcuni contratti di servizi venga effettuata la nomina a responsabile ad una organizzazione terza da parte di un titolare.

operino sotto la diretta responsabilità del responsabile o del titolare non implica anche un rapporto di lavoro dipendente. Il titolare, cioè, potrebbe nominare incaricati i dipendenti di un soggetto terzo che effettuano per suo conto alcuni trattamenti[47].
Per gli incaricati, che devono ricevere istruzioni per iscritto, il Codice richiede che, nella lettera di designazione sia individuato puntualmente l'ambito dei trattamenti consentiti che varieranno da mansione a mansione, nonché in relazione alle tipologie dei dati[48].
La designazione degli incaricati deve ritenersi valida anche se sussiste la documentata preposizione della persona fisica a una unità per la quale è individuato l'ambito del trattamento consentito agli addetti all'unità medesima. Ne consegue la validità di circolari aziendali o amministrative di nomine effettuate per categorie di dipendenti appartenenti al medesimo settore qualora l'ambito di trattamento dagli stessi eseguito sia il medesimo. E' necessario, pertanto, che esista un organigramma aziendale, completo di mansionario impostato in modo da non permettere alcuna ambiguità circa il soggetto fisico incaricato di uno specifico trattamento. Se non esiste questa ambiguità, la designazione è implicita.

TITOLO V
SICUREZZA DEI DATI E DEI SISTEMI
Capo I
Misure di sicurezza

Art. 31 Obblighi di sicurezza

Enuncia gli obblighi di sicurezza[49] cui sono tenuti tutti i titolari, sottolineando che le misure di sicurezza che verranno successivamente adottate per ridurre al minimo i rischi dovranno essere proporzionate alla tipologia di trattamento e alla natura dei dati trattati.
La adozione di idonee e preventive misure di sicurezza servono ad evitare i rischi di: 1. distruzione o perdita, anche accidentale, dei dati stessi; 2. di accesso non autorizzato; 3. di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 32 Particolari titolari

Contiene gli obblighi aggiuntivi per i titolari che forniscono " un servizio di comunicazione elettronica accessibile al pubblico[50] ".

[47] Il Garante, con una pronuncia dell'otto giugno 1999, sottolineava che se da un lato non è possibile nominare come "incaricato del trattamento" la società esterna, dall'altro non è esclusa la possibilità (ed anzi è obbligatorio) conferire l'incarico stesso ai dipendenti di detta società, i quali devono operare necessariamente sotto "la diretta autorità" del titolare o dell'eventuale responsabile del trattamento oggetto del contratto. La suddetta "autorità" si concretizza anche attraverso istruzioni periodiche.
[48] Occorrerà, quindi, fare attenzione a come verranno formulate le nomine ad incaricati, per evitare che una modifica di mansioni richieda una modifica della nomina stessa.
[49] A differenza di quanto sancito nella Direttiva 95/46/CE che prevedeva venisse effettuato un principio di bilanciamento tra costo e benefici, sia la L.n. 675/96 che il Codice non tengono conto di tale bilanciamento.

Questo articolo è dedicato in particolare ai gestori di servizi di telecomunicazione e riprende quanto contenuto in una precedente legge, per la verità mai applicata. E' fatto obbligo al titolare del trattamento di comunicare agli utenti, ad es. gli abbonati ad un gestore telefonico, le problematiche connesse alla sicurezza con la indicazione di cautele e precauzioni da adottare. (si pensi alla introduzione di programmi abusivi presso i computer degli utenti, che li connettono a numeri a pagamento, a completa insaputa degli utenti stessi).

Art. 33 Misure minime

Da rilevare che le misure minime di sicurezza non sempre sono idonee a tenere sotto controllo tutti i rischi legati al trattamento. Poiché viene confermata una sorta di responsabilità oggettiva del titolare del trattamento, in caso di violazioni di rilevanza penale nel trattamento dei dati, si tenga presente che minimo non significa idoneo.
Necessitano alcune osservazioni relativamente alle misure minime:

a. esse non rappresentano l'obiettivo di fondo cui, in teoria, un titolare dovrebbe tendere, che sono invece le "misure idonee" di cui all'art. 31;
b. l'elenco è tassativo, per cui tutte devono essere adottate, e la loro mancata adozione può comportare sia la sanzione penale[51] sia la eventuale responsabilità civile.

Nella lettura del disciplinare tecnico si vedrà che il legislatore ha ridotto la distanza tra le misure minime e le misure idonee, anche se la responsabilità finale della scelta è affidata sempre al titolare[52].
Le "misure minime" sono 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'art. 31.
Le prescrizioni dell'art. 58 si riferiscono a enti pubblici.

Art 34 Trattamenti con strumenti elettronici

Gli "strumenti elettronici" sono: gli elaboratori, i programmi per elaboratori, qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento[53].
Per i trattamenti effettuati con strumenti elettronici, il nuovo codice della privacy richiede tassativamente che:

- il sistema disponga di un **sistema di autenticazione informatica degli utenti.** Nel Dpr n. 318/99 si parlava solo di password;
- il Titolare adotti appropriate procedure, con la caratteristica della periodicità, per **mantenere aggiornate le utenze e i relativi profili di accesso** sia per gli utenti

[50] Il Codice ha recepito integralmente le prescrizioni dettate in tema di sicurezza dall'art. 4 della Direttiva 2002/58/CE.
[51] Art. 169: arresto fino a due anni o ammenda fino a cinquantamila euro.
[52] Il Titolare ed il Responsabile, per fornire la prova liberatoria di cui all'art. 2050 c.c., devono dimostrare di avere adottato tutte le misure idonee ad evitare il danno, in relazione ai seguenti parametri: conoscenze tecniche acquisite, natura dei dati trattati, caratteristiche concrete del trattamento.
[53] Le misure di sicurezza non previste nel Dpr 318/99 devono essere implementate entro il 30.6.04, a meno che le strumentazioni elettroniche del Titolare dei trattamenti siano inidonee a tale scopo: in questo caso il termine è differito a un anno dall'entrata in vigore del Codice, e sulla circostanza sarà necessario redigere un documento specifico di data certa. (art. 180)

normali sia per quelli addetti alla gestione o manutenzione dei sistemi[54]. Sia definito un **sistema di autorizzazione per abilitare gli utenti all'accesso** ai dati e/o ai trattamenti.

- Gli strumenti elettronici e i dati siano protetti da accessi non autorizzati da parte di utenti, programmi informatici e da trattamenti illeciti.
- **Il Titolare adotti un documento programmatico sulla sicurezza[55].** (Dps) che deve essere redatto entro il 31 marzo di ogni anno. La prima scadenza prevista è per il 31 marzo 2005. Nel caso sia dovuta la relazione accompagnatoria del bilancio di esercizio, il titolare ha l'obbligo di riferire in merito alla redazione o aggiornamento del Dps stesso. Per quanto riguarda i suoi contenuti, il documento rimane inalterato per la parte relativa alla distribuzione dei compiti e delle responsabilità, all'analisi dei rischi, alle misure per garantire l'integrità dei dati e la protezione delle aree e dei locali. La novità è rappresentata da: l'elenco dei trattamenti, la adozione di misure per garantire la disponibilità dei dati e il ripristino degli stessi in caso di perdita o danneggiamento. Il tempo massimo di ripristino dell'accesso ai dati deve essere compatibile con i diritti degli interessati e comunque non eccedente i sette giorni.
- sia fatto obbligo di adottare tecniche di cifratura per i trattamenti atti a rivelare lo stato di salute o la vita sessuale rilevati da organismi sanitari.
- Gli organismi sanitari devono inoltre provvedere all'adozione di:
  a. tecniche di cifratura o
  b. codici identificativi

  per determinati trattamenti di dati idonei a rivelare:
- lo stato di salute o
- la vita sessuale.

Art. 35 Trattamenti senza l'ausilio di strumenti elettronici

Per i trattamenti effettuati senza l'ausilio di strumenti elettronici si richiede che:

- la lista degli incaricati e il compito loro assegnato sia mantenuta aggiornata;
- siano definite opportune procedure per la custodia dei documenti affidati agli incaricati;
- siano definite apposite procedure per l'accesso agli archivi.

Art. 36 Adeguamento

Mentre la legge 675/96 prevedeva un aggiornamento a cadenza biennale, tale articolo stabilisce un adeguamento legato ad esigenze tecniche vista la sempre più rapida evoluzione della tecnologia.
Il Disciplinare Tecnico va aggiornato direttamente a cura del Ministero della Giustizia, in accordo col solo Ministero per le Innovazioni e le Tecnologie.

[54] I precedenti ruoli di amministratore di sistema e custode delle password non sono più previsti, ma rientrano nella categoria degli addetti alla gestione.

[55] Rispetto al Dpr 318/99, adesso il contenuto del Dps è tassativamente descritto.

Disciplinare tecnico in materia di misure minime di sicurezza.

Questo documento si articola in ventinove punti che vanno dal trattamento con strumenti elettronici al sistema di autenticazione informatica, passando per il sistema di autorizzazione e per altre misure di sicurezza. Il disciplinare raggruppa le misure minime in base a tre soli scenari:

1. trattamenti con strumenti elettronici di dati personali;
2. trattamento di dati sensibili o giudiziari;
3. trattamenti che non prevedono l'uso di strumenti elettronici.

Le modalità tecniche contenute nel disciplinare sono da adottare a cura del Titolare, del Responsabile e degli Incaricati. Nel caso in cui misure minime di sicurezza siano affidate ad una struttura esterna, questa è tenuta a fornire per iscritto, una descrizione dell'intervento effettuato che ne attesti la conformità al disciplinare tecnico

Per tutte le tipologie di trattamento sono richieste specifiche norme per istruire gli incaricati sugli aspetti critici della sicurezza, con l'intento di considerare il loro comportamento, come parte integrante delle misure di sicurezza.

Il trattamento con strumenti elettronici.

Sono undici i punti relativi al "sistema di autenticazione informatica".

* L'**autenticazione informatica** è un sistema che permette di identificare un soggetto- incaricato- non basandosi sulla conoscenza diretta o comunque percettiva, ma avvalendosi di una soluzione tecnologica[56].
* Le **credenziali di autenticazione** corrispondono ai dati ed ai dispositivi, in possesso di una persona (da questa conosciuti o ad essa univocamente correlati), utilizzati per l'autenticazione informatica. Possono essere di diverso genere: smart-card, dispositivi biometrici, ecc., ma nella maggior parte dei casi si tratta di un codice identificativo associato a una parola chiave assegnata all'incaricato.
* La **parola chiave** è una componente di una credenziale di autenticazione, un elemento associato ad una persona ed a questa noto, nella pratica una sequenza di caratteri o altri dati in forma elettronica. La password deve essere di almeno otto caratteri alfanumerici e deve essere modificata dall'interessato al primo utilizzo e poi almeno ogni sei mesi. Se si trattano dati sensibili o giudiziari la password va modificata almeno ogni tre mesi.
* Il **profilo di autorizzazione** è una specie di passaporto, su cui è scritto cosa il suo utilizzatore può vedere e quali operazioni può fare. E' l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare: a quali dati essa può accedere; i trattamenti ad essa consentiti.
* Il **sistema di autorizzazione** è l'insieme degli strumenti e delle procedure che (in funzione del profilo di autorizzazione del richiedente) abilitano l'accesso ai dati e alle modalità di trattamento degli stessi.

A differenza del precedente testo sulla sicurezza che prevedeva una diversificazione nelle misure a seconda del tipo di trattamento elettronico o meno dei dati, l'attuale ha – opportunamente – unificato le misure minime di sicurezza.

[56] L'**autenticazione informatica** è un sistema che comprende l'insieme degli strumenti elettronici e delle procedure per la verifica dell'identità o della dichiarazione di identità. A ciascuno degli incaricati, nominati con atto scritto con il quale sono impartite – anche – istruzioni sul trattamento dei dati personali, devono essere assegnate individualmente le **credenziali di autenticazione.**

1. Chiunque tratti dati personali deve essere previamente nominato incaricato e gli è permesso l'accesso a specifici dati o programmi. In altre parole, ogni incaricato deve ricevere un profilo di accesso che viene abilitato da una serie di operazioni indicate nel punto 2.
2. il testo prevede che adottando i sistemi tradizionali l'incaricato sia identificato con un codice o una parola chiave, mentre nel caso di utilizzo di dispositivi alternativi (riconoscimento biometrico, smart card, ecc.) la parola chiave possa essere omessa. Ad esempio nel caso di un dispositivo di riconoscimento biometrico la parola chiave può essere utilizzata per accelerare i tempi di ricerca nell'archivio della stringa biometrica, e non come elemento di vera e propria sicurezza.
3. tale ipotesi è di difficile attuazione, oggi si cerca di utilizzare un unico codice di identificazione ed eventualmente associare ad esso diversi profili di accesso. Le credenziali di autenticazione sono cosa diversa dal sistema di autorizzazione e servono esclusivamente a identificare l'incaricato coinvolto nel trattamento dei dati, mentre il sistema di autorizzazione serve a tracciare un quadro dei privilegi di accesso concessi ad un incaricato, debitamente autenticato ed identificato.
4. Agli incaricati devono essere fornite le opportune istruzioni perché possano adottare le cautele necessarie al fine di mantenere riservate le credenziali e/o i dispositivi in loro possesso.

5. Se viene utilizzata la parola chiave questa deve essere composta da almeno otto caratteri. Se il sistema di identificazione non preveda questa lunghezza, deve essere usata la lunghezza massima consentita. E' richiesto anche un meccanismo per evitare l'utilizzo di password comunque riconducibili all'incaricato. L'utilizzo delle password o credenziali di accesso:

- l'incaricato deve modificarle prima del primo utilizzo
- se vengono trattati dati comuni, la modifica va fata almeno ogni sei mesi
- se vengono trattati dati sensibili o giudiziari, la modifica va fatta almeno ogni tre mesi
- la parola chiave viene disattivata dopo sei mesi di mancato utilizzo, con esclusione però delle utenze dedicate alla manutenzione tecnica dei sistemi
- il titolare deve individuare precise modalità per accedere ai sistemi o ai dati, in caso di necessità, anche in assenza dell'incaricato
- la userid non può essere assegnata ad altri incaricati se non è più utilizzata.

6. il codice di identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. le credenziali di autenticazione non utilizzate da almeno 6 mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali. E' necessario, quindi, un abbinamento tra il data base dei dipendenti e l'archivio degli incaricati.
9. E' frequente il caso in cui un incaricato si allontani dal proprio terminale, lasciandolo attivo ed abilitato, e quindi a disposizione per un eventuale accesso abusivo. Occorre, pertanto, predisporre screen savers sotto password, che si attivano automaticamente dopo pochi minuti di inattività del terminale.
10. Se l'incaricato che ha titolo all'accesso non è disponibile ed è necessario accedere a questi dati, è prescritto che venga attivata una procedura, grazie alla quale sia comunque possibile recuperare la parola chiave, esclusivamente detenuta dall'incaricato in questione, per potere accedere ai dati stessi. L'incaricato non appena riprenderà il servizio dovrà modificare la password.

11. quando il dato è destinato alla diffusione non è indispensabile attuare specifiche misure di controllo dell'accesso al dato stesso.

SISTEMA DI AUTORIZZAZIONE

12. Se un incaricato deve potere accedere con diversi profili a diverse categorie di dati allora è utilizzato un sistema di autorizzazione. Ad es. quando un incaricato può accedere ad un dato ma non abbia il potere di modificarlo, una volta introdotto nel sistema. I diversi livelli di autorizzazione all'accesso, alla modifica ed alla cancellazione devono essere rispecchiati da specifici profili di autorizzazione, gestiti da una apposita procedura.

13. i profili di accesso, da assegnare a ogni incaricato, devono essere predisposti in anticipo rispetto all'inizio del trattamento e consentire l'accesso solo ai dati necessari per effettuare le specifiche operazioni di trattamento.

14. Va effettuata una verifica periodica, almeno annuale, della necessità di mantenere per gli incaricati il relativo profilo di accesso.

15. E' previsto l'aggiornamento, almeno annuale, per ogni trattamento, della lista degli incaricati, degli addetti alla gestione e manutenzione degli strumenti elettronici nel loro complesso. La lista può essere redatta anche per classi omogenee di incarico e dei relativi profili di accesso.

16. Rischio da intrusione, art. 615 – quinquies del c.p., l'aggiornamento è semestrale. E' previsto l'aggiornamento annuale per i dati comuni e semestrale per quelli sensibili o giudiziali, delle patch di sicurezza per i programmi e i sistemi.

17. Il titolare del trattamento ha l'obbligo di aggiornare periodicamente i dati personali e il responsabile ha l'obbligo di aggiornare periodicamente i programmi e i sistemi operativi.

18. E' obbligatorio il salvataggio dei dati a cadenza almeno settimanale, secondo definite istruzioni organizzative e tecniche. La presenza di questo punto consente agli ispettori del Garante di effettuare una verifica ben più incisiva della efficienza ed efficacia con cui vengono rispettate le disposizioni del disciplinare, in fase di ispezione.

19. contiene la prescrizione, a carico del titolare di un trattamento di dati sensibili o giudiziari, di redigere il documento una volta l'anno, anche attraverso il responsabile se designato. Chiunque utilizza un sistema informativo che tratti dati personali deve allestire un organigramma funzionale della struttura informatica, che gestisce tali dati. Il documento programmatico della sicurezza deve essere completato da una descrizione delle funzioni e delle responsabilità di tutti i soggetti fisici o delle entità organizzative, che concorrono al trattamento dei dati. Qualsiasi programma di protezione deve partire dall'analisi dei rischi che incombono sui dati stessi e, pertanto, devono essere previsti interventi formativi degli incaricati in proposito. Per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, vanno adottate misure di protezione particolari, comunque, superiori a quelle garantite a dati personali di natura non sensibile[57].

20. i dati sensibili e giudiziari devono essere protetti in modo particolare, delegando al titolare del trattamento, al suo responsabile, la scelta di strumenti che possono essere ritenuti "idonei". Occorre prevedere il rischio di intrusione di cui all'art. 615 –ter del c.p.

[57] Occorre che sia chiarito meglio il requisito della separazione dei dati dagli altri dati personali in quanto, prima o poi, i dati per qualche ragione dovranno essere aggregati. La interpretazione corretta dovrebbe essere che i dati idonei a rivelare lo stato di salute debbano, nella norma, essere tenuti separati dagli altri; quando invece sia richiesto da necessità non derogabili, per esempio connesse ad adempimenti specificamente richiesti da norme di legge o di contratto, solo allora possano essere riconnessi agli altri.

21. l'uso e la custodia dei supporti rimovibili devono essere regolamentati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimuovili, se non più utilizzati, vanno distrutti.
23. E' obbligatorio attuare piani di disaster recovery e di backup, per garantire il ripristino dell'accesso ai dati in caso di danneggiamento, in tempi compatibili.
24. Il testo impone, per la prima volta, che i supporti dei dati – trasferiti tra strutture sanitarie – debbano essere protetti in contenitori muniti di serratura. Mentre se il trasferimento avviene con canali di telecomunicazione o con supporti, su cui sono registrati dati informatizzati, il trasporto deve avvenire su supporti cifrati.
25. In caso di outsourcing devono essere indicati i criteri da adottare per garantire l'adozione delle misure minime di sicurezza. La prescrizione del legislatore mette in evidenza specifica il fatto che l'affidamento a terzi di dati personali, nel quadro di un rapporto di con titolarità del trattamento, di responsabile del trattamento o di incaricato del trattamento, comporta un coinvolgimento pieno sia di chi affida i dati da trattare, sia di chi tratta i dati ad esso affidati. Ecco perché nel documento programmatico deve essere previsto uno specifico capitolo, nel quale vengono presi in considerazione tutti gli aspetti di sicurezza, legati al trattamento di dati che sono affidati a soggetti esterni, quale che sia il tipo di rapporto, nell'ambito del quale sono affidati.
26. Le spa devono presentare unitamente al bilancio di esercizio anche una dichiarazione, circa l'avvenuta redazione o avvenuto aggiornamento del documento programmatico della sicurezza.

IL TRATTAMENTO DEI DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI.

27. Per i dati comuni basta che agli incaricati siano impartite istruzioni per iscritto, con riferimento all'intero ciclo del trattamento, che quindi devono essere reperibili e documentabili a richiesta degli ispettori del Garante.. Non è più previsto l'obbligo di conservare i documenti in archivi ad accesso selezionato.
28. Gli incaricati ai quali sono affidati documenti con dati sensibili o giudiziari devono custodirli ed evitare che personale non autorizzato acceda agli stessi. Al termine del trattamento i documenti devono essere restituiti. Non è più richiesto l'obbligo dei contenitori muniti di serratura.
29. Permane l'obbligo di identificare e registrare l'accesso, fuori orario, agli archivi con dati sensibili o giudiziari e l'autorizzazione preventiva in caso di vigilanza.

Il calendario con le date relative all'adozione delle misure di sicurezza:

Adempimento	Scadenza
Misure di sicurezza idonee o di base e misure minime previste dal Dpr 318/99	già in vigore
Nuove misure minime di sicurezza non previste dal Dpr 318/99	**31 dicembre 2005**

Differimento per impossibilità tecnica di poter adottare le misure minime di entro la scadenza	31 marzo 2006
Predisposizione del documento programmatico sulla sicurezza	31 marzo di ogni anno

TITOLO VI
ADEMPIMENTI

Art. 37 Notificazione del trattamento

La notificazione[58] è una dichiarazione con la quale un soggetto pubblico o privato rende noto al Garante le caratteristiche principali del trattamento dei dati personali eseguito da parte del "Titolare".

La ratio legis sottostante all'introduzione dell'obbligo di notificazione è quella di consentire al Garante un controllo di conformità in merito alle operazioni che si effettuano sui dati e la possibilità per chiunque di accedere alle informazioni che la compongono, mediante il pubblico registro dei trattamenti tenuto presso il Garante[59].

L'obbligo di notificazione[60] va adempiuto in via preliminare rispetto al trattamento che ha richiesto l'adempimento e va ripetuto, sempre in via preventiva, solo:

a) prima che cessi definitivamente l'attività di trattamento; o

b) prima che si apportino al trattamento alcune modifiche agli elementi da indicare nella notificazione.

La precedente normativa prevedeva un sistema "in positivo", nel senso della sussistenza di un obbligo generale di notificazione, salvo le eccezioni espressamente previste. L'attuale riforma, invece, non prevede più l'obbligo di notificazione salvo che il trattamento posto

[58] L'obbligo nasce con la legge 676/96 ed è estensivo: devono essere notificate al Garante determinate categorie di trattamenti di informazioni personali. L'obiettivo è quello di creare un registro delle notificazioni. Ci si rende, però, immediatamente conto che l'obiettivo è azzardato e si decide di prevedere una lunga serie di esenzioni. Alla fine il risultato è che devono essere notificati tutti i trattamenti, ad eccezione di quelli espressamente indicati dalla nuova disposizione. Il Codice della privacy ribalta il principio: al Garante devono essere notificati solo i trattamenti elencati nell'art. 37. per tutti gli altri l'obbligo cade.

[59] Tale registro a oggi non risulta ancora costituito.

[60] Per le attività di trattamento dei dati che non esistevano prima del 1° gennaio 2004, la notificazione va effettuata prima che inizi il trattamento medesimo. Per le attività che erano già in essere prima del 1° gennaio 2004, la notificazione si può effettuare entro il 30 aprile 2004.

in essere da parte dei "titolari" sia connotato dagli elementi espressamente previsti dal legislatore.

Tale articolo prevede l'obbligo di procedere alla notificazione al Garante in quelle situazioni in cui le particolari modalità di trattamento o la natura dei dati personali facciano ritenere che sussistano potenziali rischi per la riservatezza e la dignità dell'individuo.

Alla luce della delibera del Garante, dell'aprile 2004, i casi attualmente previsti sono[61]:

1. la raccolta di dati genetici, biometrici[62]o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica[63]; a tale proposito si deve ritenere che siano soggetti a notifica quei sistemi che consentono la identificazione geografica di oggetti, solo quando questi siano associati a persone (fisiche o giuridiche) identificate o identificabili; diversamente si avrebbe un trattamento di dati che non sono personali, in quanto riferiti solo ad oggetti, es un pacco, senza che ad essi sia applicabile la legge;
2. i 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[64] - solo se relativi ad una

[61] L'articolo 37 si rivela, ben presto, impreciso in quanto le categorie dei dati individuati dalla norma sono troppo estesi e, costringe, molti soggetti a chiedere chiarimenti al Garante il quale, grazie al dettato dello stesso articolo che prevede la possibilità di un suo intervento per accrescere o snellire la lista dei titolari soggetti a notificazione con una apposita delibera, ha chiarito molti dubbi.

[62] Non sono soggetti a notificazione: i trattamenti non sistematici di dati genetici o biometrici effettuati da **esercenti le professioni sanitarie**, anche unitamente ad altri esercenti titolari dei medesimi trattamenti rispetto a dati non organizzati in una banca dati accessibile a terzi per via telematica. Ciò limitatamente ai dati e alle operazioni, compresa la comunicazione, indispensabili per perseguire finalità di tutela della salute o dell'incolumità fisica dell'interessato o di un terzo. L'obbligo della notificazione, invece, resta per i trattamenti genetici e biometrici effettuati da strutture sanitarie pubbliche o private: ospedali, case di cura o di riposo, centri di riabilitazione, ambulatori polispecialistici, laboratori di analisi cliniche e di diagnostica per immagini, studi fisioterapici, aziende sanitarie, istituti clinici privati, associazioni sportive.

Stesso discorso vale per gli **avvocati**.

[63] La norma si riferisce alla localizzazione di persone o oggetti, ed è quindi riferita alla rilevazione della loro presenza in determinati luoghi, mediante reti di comunicazione elettronica gestite o accessibili dal titolare del trattamento. Alla luce delle deliberazione del Garante n. 1/2004, la localizzazione va notificata quando permette di individuare in maniera continuativa, anche con eventuali intervalli, l'ubicazione sul territorio o in determinate aree geografiche, in base ad apparecchiature o dispositivi elettronici detenuti dal titolare o dalla persona oppure collocati sugli oggetti. La localizzazione deve comunque permettere di risalire alla identità degli interessati, anche indirettamente attraverso appositi codici. Non devono quindi essere notificati al Garante i trattamenti di dati personali che consentano solo una rilevazione non continuativa del passaggio o della presenza di persone o oggetti, effettuata, ad es., all'atto della: a) registrazione di ingresso o uscite presso i luoghi di lavoro; b) rilevazione di immagini o suoni, anche con impianti a circuito chiuso, presso immobili o edifici ove si svolgono attività del titolare del trattamento a meno che, anche mediante interazione con altri sistemi, il titolare possa rilevare le diverse ubicazioni o spostamenti di una persona o di un oggetto in determinati luoghi o aree sul territorio.

[64] Non sono soggetti a notificazione i trattamenti di dati idonei a rivelare lo stato di salute e la vita sessuale effettuati da esercenti le professioni sanitarie, anche unitamente ad altri esercenti

banca dati o alla fornitura di beni -; e' tenuto alla notificazione chi eroga servizi sanitari per via telematica relativi a una banca di dati o alla fornitura di beni. Sono invece esonerati i seguenti trattamenti: quelli effettuati nel contesto della teleassistenza, quelli che presuppongono b.d. informatizzate, ma senza che i pc siano collegati ad una rete telematica; quelli alla cui base ci sono archivi cartacei. Non devono essere quindi notificati i trattamenti di dati sanitari, e/o sulla vita sessuale, effettuati nell'ambito di servizi di assistenza o consultazione sanitaria per via telefonica, come i servizi telefonici gestiti in ambito assicurativo e che consentono il consulto di esercenti le professioni sanitarie. Per quanto riguarda le malattie mentali, si devono notificare solo i trattamenti effettuati "ai fini di rilevazione" di quelle patologie[65].

3. dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro; trattasi di una novità assoluta, che suscita perplessità per la sua indeterminatezza[66];
4. la definizione di profili con strumenti elettronici[67]; per profilazione il legislatore intende praticamente tutto: dai dati relativi allo svolgimento di attività economiche a quelli relativi all'adempimento di obbligazioni, ecc.;
5. la gestione di dati sensibili da parte di agenzie di ricerca di personale per conto terzi[68];
6. la gestione di banche dati per rischi creditizi o antifrode.

Il codice della privacy ha riconosciuto il potere del Garante di modificare, per difetto o per eccesso, con proprio provvedimento, l'elencazione attualmente contenuta nella legge, come casistiche per le quali si rende obbligatoria la notificazione.

---

titolari dei medesimi trattamenti: **a)** a fini di procreazione assistita, di trapianto di organi e di tessuti, indagine epidemiologica, rilevazione di malattie mentali, infettive, diffusive o di sieropositività. Ciò sempre che i trattamenti siano effettuati non sistematicamente, rispetto a dati non organizzati in una banca dati accessibile a terzi per via telematica e limitatamente ai dati e alle operazioni indispensabili per la tutela della salute o dell'incolumità fisica dell'interessato o di un terzo.**b)** a esclusivi fini di monitoraggio della spesa sanitaria o di adempimento di obblighi normativi in materia di igiene e sicurezza del lavoro e della popolazione. Sono esonerati dalla notificazione, anche, i medici specialisti che trattano i dati sulla procreazione assistita nell'ambito dell'attività di consulenza o quelli che utilizzano le informazioni sulla sieropositività in relazione al sistema di sorveglianza epidemiologica nazionale dei casi di Aids conclamato.

[65] Niente notificazione, dunque, in occasione di episodi occasionali di diagnosi e cura o quando, per esempio, in un Comune bisogna adottare un provvedimento di trattamento sanitario obbligatorio.

[66] Il Garante, con Deliberazione n. 1/04, ha precisato che rimangono esclusi dalla notifica tutti i trattamenti effettuati da associazioni sindacali ed enti non lucrativi, al solo fine di adempiere agli obblighi previsti dalla normativa sul lavoro o sulla previdenza sociale.

[67] Sono esonerati dall'obbligo di notificare i trattamenti effettuati al fine di definire e verificare le attitudini del personale, purchè non vengano utilizzati esclusivamente sistemi automatizzati. Questa condizione comporta che, per essere esonerato dalla notificazione, il datore non deve limitarsi ad impiegare nella fase valutativa soltanto mezzi automatizzati (come le schede a lettura ottica), ma anche personale che deve partecipare attivamente all'attività.

[68] Sono escluse dalla notificazione i trattamenti effettuati ai fini di selezione per conto di soggetti appartenenti al medesimo gruppo societario. Quindi la condizione per l'esonero dalla notificazione è che la selezione sia affidata a una società facente parte del medesimo gruppo di quella che ha esternalizzato tale attività.

I trattamenti esclusi dall'obbligo di notificazione devono però essere resi conoscibili per cui i loro titolari debbono fornire a chiunque ne faccia richiesta gli elementi contenuti nel modello predisposto dal Garante per la notificazione. La norma esclude la necessità di un interesse qualificato del richiedente.
L'omissione o la incompletezza sono punite con sanzioni amministrative congiunte: pagamento di una somma[69] e pubblicazione dell'ingiunzione di pagamento.
La falsità nella notificazione costituisce reato punibile con la reclusione.
Per i trattamenti dei dati personali iniziati prima del 1.1.2004, in sede di applicazione del presente Codice, le notificazioni previste dall'art. 37 sono effettuate entro il 30 aprile 2004.

Art. 38 Modalità di notificazione

Il termine per presentare la notificazione al Garante è il 30 aprile per i trattamenti iniziati prima del 1° gennaio 2004 – anche se già notificati vigente la legge 675/96 – mentre i nuovi trattamenti devono essere comunicati all'Autorithy prima del loro inizio.
La notificazione è una dichiarazione per la quale è prevista dal legislatore una determinata forma e specifiche modalità di trasmissione:

a) deve essere rilasciata secondo il modello messo a disposizione dal Garante e contenere le informazioni in esso richieste;
b) deve essere trasmessa per via telematica, previa apposizione della firma digitale[70] da parte del dichiarante; con la firma digitale è stato introdotto un requisito di validità formale che è aggiuntivo rispetto al passato e contrasta con la prevista semplificazione;
c) secondo le prescrizioni impartite dall'Autorità.

Da rilevare che, in base al comma 6, chiunque potrà richiedere al Titolare, anche se quest'ultimo non è tenuto alla notifica, le notizie richieste dal modulo di notifica predisposto dal garante. Il che vuol dire che chiunque, cioè non solo i soggetti interessati, potrà imporre a chiunque di fornire quelle notizie che, invece, il Garante non ritiene di dovere più richiedere!

Art. 39 Obblighi di comunicazione

Tale articolo ha introdotto un obbligo di comunicazione al Garante da assolvere nelle seguenti fattispecie:

1. quando un ente pubblico comunichi ad un altro ente pubblico dati personali di terzi in casi non previsti da norma di legge o di regolamento;
2. quando venga effettuato un trattamento di dati relativi allo stato di salute a scopi di ricerca sanitaria, nei casi in cui non è necessario il consenso dell'interessato ex art. 110, comma 1.

Questi trattamenti possono essere iniziati solo dopo 45 giorni dal ricevimento della comunicazione da parte del Garante[71] allo scopo di consentirgli di valutare la necessità di eventuali provvedimenti in merito.

---

[69] Da 10 mila euro a 60 mila euro.
[70] Il legislatore richiama le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione anche se, più correttamente, avrebbe dovuto riferirsi alla firma elettronica e non a quella digitale.
[71] Anche in questi casi è il Garante a fornire un apposito modello da compilare e da trasmettere per via telematica, con firma elettronica, o con fax o raccomandata A/R.

Art. 40 Autorizzazioni generali

Con le autorizzazioni generali, l'Autorità acconsente a operazioni di trattamento di dati sensibili o giudiziari a determinate condizioni e per determinati fini.
Per consentire la rapida circolazione delle informazioni, il Garante ha rilasciato delle autorizzazioni generali per tipologie di trattamenti, con le quali sono stati legittimati alcuni trattamenti di dati sensibili o giudiziari analiticamente specificati.
Le autorizzazioni generali[72] sono pubblicate sulla G.U. al fine di darvi la massima diffusione e conoscibilità. Le autorizzazioni attualmente "vigenti" esplicheranno i loro effetti giuridici fino al giugno 2004.

Art. 41 Richieste di autorizzazione

Nel caso ci si trovi in una delle situazioni già previste e acconsentite nelle autorizzazioni generali, il "titolare" non sarà tenuto a presentare specifica richiesta di autorizzazione al Garante.
Nel caso, invece, in cui lo specifico trattamento che il titolare intende porre in essere non è contemplato e autorizzato nelle menzionate autorizzazioni generali sussisterà in capo al titolare l'obbligo di sottoporre, in via preventiva rispetto all'inizio del trattamento dei dati, una dettagliata richiesta di autorizzazione al Garante tramite la compilazione di uno specifico modulo rilasciato dall'Autorità stessa.
Nell'ipotesi in analisi non vige il principio del silenzio assenso della pubblica amministrazione, previsto nella ipotesi di comunicazione al garante, posto che la mancata pronuncia entro detto termine equivale a rigetto.
Il rispetto delle formalità, talvolta, costituisce un vero presupposto giuridico per l'ammissibilità della richiesta.

TITOLO VII
TRASFERIMENTO DEI DATI ALL'ESTERO

La normativa comunitaria nel settore del trattamento dei dati è stata attenta nel contemperare le esigenze di protezione della dignità della persona e della privacy con le necessità connesse alla libera circolazione dei dati essenziali nella concreta realizzazione di un libero mercato.

Art. 42 Trasferimenti all'interno dell'Unione europea

Al fine di assicurare la libera circolazione dei dati è stabilito un limite generale all'interpretazione per gli operatori giuridici e per gli interessati dalla normativa in esame, stabilendo l'impossibilità di un'applicazione che determini una restrizione alla libera circolazione dei dati personali tra Stati membri o che comporti addirittura un divieto generale. L'unica possibile restrizione all'indicata libertà si consente nel caso di

[72] L e **autorizzazioni** rappresentano lo strumento più idoneo per assicurare agli interessati uniformità ed effettività di garanzie e, al contempo, permettono al titolare del trattamento di prescindere dalla richiesta di autorizzazione.

"trasferimenti di dati effettuati al fine di eludere le medesime disposizioni", mentre per i trasferimenti verso Paesi terzi si richiede che lo Stato sia in grado di assicurare "una protezione adeguata".

Art. 43 Trasferimenti consentiti in Paesi terzi

Tale tipo di trasferimento, anche se temporaneo, "è vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato", tale operazione è consentita solo quando alternativamente:

- l'interessato abbia manifestato il proprio consenso espresso e, se si tratta di dati sensibili, lo abbia fatto in forma scritta;
- sia necessaria per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato;
- sia necessaria per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento o, se il trasferimento riguardi dati sensibili o giudiziari, specificato o individuato ai sensi degli artt. 20 e 21 del Codice;
- sia necessaria per la salvaguardia della vita o della incolumità fisica di un terzo;
- sia necessaria ai fini dello svolgimento delle investigazioni difensive di cui alla L.n. 397/2000 o per fare valere o difendere un diritto in sede giudiziaria;
- sia effettuata in accoglimento di una richiesta di accesso ai documenti amministrativi;
- sia necessaria, in conformità ai rispettivi codici di deontologia per esclusivi scopi scientifici o statistici;
- il trattamento concerna dati riguardanti persone giuridiche, enti o associazioni.

Qualora non si rientri in questa casistica, occorrerà presentare richiesta al Garante, che dovrà emettere provvedimento autorizzativi.

Art. 44 Altri trasferimenti consentiti

Al di là di queste ipotesi può comunque procedersi al trasferimento di dati personali all'estero quando l'operazione autorizzata dal Garante nei casi in cui abbia individuato adeguate garanzie per i diritti dell'interessato o quando siano stati individuati dalla Commissione Europea livelli di protezione adeguati forniti da Paesi extra U.E. e quando apposite clausole contrattuali offrano sul tema garanzie sufficienti.

PARTE II
DISPOSIZIONI RELATIVE A SPECIFICI SETTORI

Tali disposizioni attengono ai trattamenti di dati effettuati:

- in ambito giudiziario[73], artt. 46-52;

[73] Il Titolo I della Parte I del Codice detta le disposizioni normative inerenti ai dati personali in ambito giudiziario, riconoscendo quali soggetti Titolari del relativo trattamento gli Uffici

- delle forze di polizia[74], artt. 53-57;
- degli organismi per le informazioni e la sicurezza dello Stato[75].

Si tratta di fattispecie nelle quali vengono in rilievo esigenze superiori di tutela della collettività intera; queste esigenze giustificano la compressione dei diritti sui dati personali. In questi ambiti non rileva la distinzione tra dati comuni e sensibili.
Le "disposizioni specifiche" si sovrappongono sia alle "disposizioni generali" applicabili a tutti i trattamenti, sia alle "regole ulteriori" applicabili in ambito pubblico, per integrarle o, solo ove espressamente previsto, per sostituirle o renderle inapplicabili nello specifico caso contemplato (art. 6)

TITOLO IV
TRATTAMENTI IN AMBITO PUBBLICO

Capo I
Accesso a documenti amministrativi

Art. 59 Accesso ai documenti amministrativi

Il nuovo codice della privacy appare ispirato da una logica di semplificazione allorché dedica una apposita disposizione al trattamento dei dati comuni, sensibili e giudiziari in riscontro ad una istanza di accesso ai sensi della L.n. 241/90 e successive modificazioni, nonché delle altre disposizioni di legge in materia e dei relativi regolamenti di attuazione, sancendo la supremazia di tale disciplina, e risolvendo il conflitto attraverso il sostanziale rinvio alla fonte regolamentare[76].

---

giudiziari di ogni ordine e grado, il CSM e il Ministero della Giustizia relativamente alle rispettive attribuzioni conferite per legge o per regolamento.

[74] Il Titolo II della Parte II del Codice è dedicato al trattamento dei dati personali da parte del Centro Elaborazione Dati del Dipartimento di pubblica sicurezza o da forze di polizia.

[75] Quando il trattamento è effettuato dal CESIS, dal SISMI o dal SISDE, o ha per oggetto dati coperti dal segreto di Stato o è posto in essere da soggetti pubblici per finalità di difesa o di sicurezza dello Stato in base ad espresse disposizioni di legge che prevedano specificamente il trattamento, si applicano solo le seguenti disposizioni del Codice: articoli da 1 a 6, 11, 14, 15, 31, 33, 58, 154, 160 e 169.

[76] Tale articolo individua la l.n. 241/90 come fonte regolatrice sostanziale e processuale dell'accesso ai documenti ammnistrativi anche giudiziari e sensibili, eccezion fatta per i documenti contenenti dati sullo stato di salute e la vita sessuale. I limiti all'accesso vanno quindi ricercati all'interno delle disposizioni cui rimanda il Codice. La L.n. 241/90, all'art 24, comma 2, lett. d) esclude il diritto all' accesso quando violi la riservatezza di terzi a meno che l'accesso medesimo sia necessario per la difesa di un interesse giuridico del richiedente; in tal caso deve essere garantita la **visione** dei documenti richiesti. Il Dpr n. 352/92, all'art. 8, specifica i criteri cui si devono attenere le P.A. per regolamentare l'esercizio del diritto di accesso, che deve essere negato quando contrasti con l'esigenza di tutelare la riservatezza di terzi, con riferimento particolare ad una serie di interessi quale quello **sanitario** per quanto attiene al proprio stato di salute. Ma se al richiedente necessita l'accesso ad atti relativi a

La disposizione appare considerare tre distinti parametri di giudizio, al fine di consentire l'ostensione (= accesso) di documenti amministrativi che comprendano dati super-sensibili di terzi interessati, rispettivamente allorché:

1. la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso sia di rango almeno pari ai diritti dell'interessato. In tal caso, il confronto va condotto con riferimento alla concreta valenza delle contrapposte situazioni soggettive di riferimento;
2. la situazione giuridicamente rilevante consista in un diritto della personalità.
3. la situazione giuridicamente rilevante consista in un altro diritto o libertà fondamentale o inviolabile.

Art. 60 Dati idonei a rivelare lo stato di salute e la vita sessuale

L'accesso a documenti contenenti dati sulla salute o la vita sessuale di terzi può essere soddisfatto soltanto se la situazione giuridica che il richiedente intende tutelare è di rango almeno pari al diritto alla riservatezza del controinteressato.
Il Codice ha quindi confermato la disposizione di cui all'art. 16, comma 2, del D.Lgs.vo n. 135/99 che considera di "rilevante interesse pubblico" i trattamenti di dati sensibili effettuati per fare valere il diritto di difesa da parte del richiedente, sia in sede amministrativa che giudiziaria, con una sola eccezione: quando il trattamento riguarda dati idonei a rivelare lo stato di salute o la vita sessuale di terzi, è consentito solo se il diritto da difendere è dello stesso rango dell'interessato.
In ogni caso, l'accesso dovrà essere consentito nei limiti previsti dalle leggi e dalle disposizioni regolamentari in materia (art.16.c.1,lett.d) del D.Lgs.vo n.135/99): potrà quindi essere ammessa solo la visione e non l'estrazione di copia della documentazione clinica.

TITOLO V
TRATTAMENTO DI DATI PERSONALI IN AMBITO SANITARIO[77]

Capo I
Principi generali

Art. 75 Ambito applicativo

---

procedimenti amministrativi per tutelare propri interessi giuridici, la loro visione deve essere garantita.

[77] La disciplina è articolata secondo uno schema per cui al Capo I (artt. 75 e 76) vengono indicati i principi generali; nel Capo II (artt. 77-84) le modalità semplificate per informativa e consenso; nel Capo III (artt. 85 e 86) sono definite e chiarite le rilevanti finalità di interesse pubblico; nei Capi IV, V, e VI (artt. 87-94) sonodisciplinate le prescrizioni mediche, i trattamenti di dati genetici e altre ipotesi.

Il trattamento dei dati personali in ambito sanitario è oggetto di una disciplina minuziosamente dettagliata al fine di assicurare adeguati standard di sicurezza e rispetto della privacy a quanti si rivolgono presso le strutture sanitarie per finalità di controllo, prevenzione e cura delle malattie.

Art. 76 Esercenti professioni sanitarie e organismi sanitari pubblici

Il trattamento dei dati idonei a rivelare lo stato di salute è consentito con il consenso scritto dell'interessato e l'autorizzazione del Garante (art. 26).
L'art. 76 prevede due ipotesi che derogano a tale principio generale e che consentono il trattamento dei dati idonei a rivelare lo stato di salute quando sussista solo uno di tali requisiti:

a. con il consenso dell'interessato ma senza l'autorizzazione del Garante; e
b. senza il consenso dell'interessato ma con l'autorizzazione del Garante.

Altra eccezione è contenuta nel comma 4, lett. b) dell'art. 26, che prevede la non obbligatorietà del consenso, ma si richiede comunque l'autorizzazione del Garante, nel caso di trattamenti necessari per la incolumità di un terzo o, se si tratta dell'interessato, quando costui non sia in grado di esprimere il suo consenso perché incapace di intendere o di volere. In tal caso il consenso è espresso da un familiare o dal responsabile della struttura ove dimora l'interessato[78].
Altro caso di eccezione alla regola generale riguarda l'ipotesi prevista dall'art. 110 per il quale non è necessario il consenso per il trattamento dei dati idonei a rivelare lo stato di salute finalizzato a scopi di ricerca quando la ricerca stessa sia prevista da un'espressa disposizione di legge che prevede specificamente il trattamento, o rientra in un programma di ricerca biomedica o sanitaria prevista ai sensi del D.Lgs.vo n. 502/92 e per il quale sono decorsi 45 giorni dalla comunicazione al Garante ai sensi dell'art. 39.

Art 77 Casi di semplificazione

La consapevolezza della complessità delle disposizioni di legge porta ad individuare modalità semplificate, in grado di coniugare le necessità amministrative connesse alle prestazioni sanitarie con i diritti del cittadino, in modo particolare per quanto riguarda due problemi: la informativa dovuta all'interessato e la manifestazione del consenso. Tali modalità sono applicabili da tre categorie di soggetti:

a) dagli organismi sanitari pubblici;
b) dagli altri organismi privati e dagli esercenti le professioni sanitarie;
c) dai servizi di soggetti pubblici operanti in ambito sanitario o della prevenzione e sicurezza del lavoro.

Art. 78 Informativa del medico di medicina generale o del pediatra

Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente ai dati personali, in forma chiara e tale da rendere facilmente comprensibili gli

[78] In questi casi trova applicazione il consenso successivo, di cui all'art. 82, comma 2.

elementi previsti dalla legge. L'elemento innovativo è che l'informativa è valida per il complessivo trattamento dei dati personali necessario per l'attività sanitaria svolta dal medico, nonché per ogni trattamento correlato, effettuato dal medico che sostituisce temporaneamente il medico o il pediatra, da chi fornisce la richiesta prestazione specialistica, da chi può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata, da chi fornisce i farmaci prescritti[79]. E' di regola fornita per riscritto, anche attraverso specifica documentazione, e deve contenere non solo gli elementi richiesti dalla legge, ma anche elementi aggiuntivi collegati a eventuali trattamenti di dati che avvengano per scopi scientifici, nell'ambito di attività di tele assistenza e telemedicina e di servizi forniti attraverso reti di comunicazione elettronica. Deve inoltre indicare i trattamenti che presentino rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, effettuati per scopi di ricerca scientifica o di sperimentazione clinica, o nell'ambito di servizi di tele assistenza e tele medicina, o per fornire beni e servizi attraverso una rete informatica.

Art. 79 Informativa da parte di organismi sanitari

Gli organismi sanitari pubblici e privati si avvalgono delle medesime modalità semplificate, per cui l'informativa, una volta fornita, vale per la pluralità di prestazioni erogate anche da distinti reparti e unità dello stesso organismo o di più strutture ospedaliere e territoriali specificamente identificati. E' importante che l'organismo o le strutture annotino l'avvenuta informativa con modalità uniformi e con adeguate misure organizzative per consentirne la verifica anche da parte di altri reparti e in tempi diversi, nonché l'utilizzo per più trattamenti.
Anche i competenti servizi o strutture di soggetti pubblici operanti in ambito sanitario o della prevenzione e sicurezza del lavoro possono avvalersi della facoltà di fornire un'unica informativa per una pluralità di trattamenti effettuati.
Cartelli idonei e avvisi visibili al pubblico devono integrare l'informativa fornita dagli organismi sanitari, facendo meglio conoscere le finalità della legge sulla privacy e soprattutto i diritti del cittadino.

Art. 80 Informativa da parte di altri soggetti pubblici

I servizi o le strutture di soggetti pubblici operanti in ambito sanitario o della prevenzione e sicurezza del lavoro hanno la facoltà di fornire un'unica informativa per una pluralità di trattamenti e per dati raccolti presso l'interessato o presso terzi.

Art. 81 Prestazione del consenso

Circa le modalità di manifestazione del consenso il codice della privacy stabilisce due criteri:

[79] Se il medico che ha fornito la informativa ed ottenuto il consenso, nel corso della terapia ritenesse di richiedere l'intervento di uno specialista o di prescrivere un farmaco, loo specialista e il farmacista sono soggetti coperti dalla informativa originariamente fornita dal medico di base-pediatra. Se, invece, per quella stessa malattia si rendesse necessario il ricovero in ospedale, la informativa del medico di base avrebbe esaurito la sua area di validità; sarà l'ospedale a dovere predisporre una nuova informativa e acquisire un nuovo consenso. Il Codice stabilisce per entrambe le ipotesi di informativa e di consenso semplificati il principio della verifica successiva sia per gli organismi sanitari pubblici sia privati.

a) il consenso al trattamento dei dati sensibili (=idonei a rivelare lo stato di salute) può essere manifestato con una unica dichiarazione, sia per iscritto che oralmente;
b) nel caso di manifestazione orale, il consenso è documentato con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico, da cui risulti anche l'informativa resa all'interessato[80]. Qualora il medico o il pediatra forniscano l'informativa per conto di altri professionisti, devono essere adottate idonee modalità per rendere conoscibile anche il consenso. I medici di medicina generale e i pediatri di libera scelta dovranno acquisire il consenso degli assistiti entro il 30 settembre 2004.

Art. 82 Emergenze e tutela della salute e dell'incolumità fisica

L'informativa e il consenso al trattamento dei dati personali possono intervenire senza ritardo, successivamente alla prestazione:

1. per l'emergenza sanitaria o di igiene pubblica[81];
2. nel caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile acquisire il consenso di chi esercita legalmente la potestà, da un prossimo congiunto, da un familiare, da un convivente, o in loro assenza, dal responsabile della struttura presso cui dimora l'interessato;
3. nel caso di rischio grave, imminente e irreparabile per la salute o l'incolumità fisica dell'interessato[82];
4. in caso di prestazione medica, che può essere pregiudicata dall'acquisizione preventiva del consenso, in termini di tempestività o efficacia.

Art. 83 Altre misure per il rispetto dei diritti degli interessati

Sono elencate una serie di misure che i soggetti sopraindicati (organismi pubblici e privati, esercenti le professioni, singole strutture o servizi) devono adottare a tutela delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale: sono soprattutto interventi organizzativi, cautele procedimentali, aggiornamenti di procedure che possono agevolare l'applicazione della legge. In particolare ricordiamo:

- ordini di precedenza e di chiamata per prestazioni, che prescindano dall'individuazione nominativa dei soggetti; i medici di medicina generale e per i pediatri di libera scelta potranno, invece, convocare gli assistiti per nome.

[80] Sorge il dubbio se il soggetto che effettua la documentazione del consenso sia o diventi un pubblico ufficiale e, di conseguenza, se la certificazione relativa alla acquisizione del consenso sia o meno atto pubblico. A ben vedere chi certifica l'avvenuta manifestazione del consenso non deve essere un pubblico ufficiale perché tale requisito non è richiesto dalla norma.

[81] In tali ipotesi le ordinanze con tingibili e urgenti sono adottate dal sindaco, quale rappresentante della comunità locale. Negli altri casi dei provvedimenti d'urgenza spetta allo Stato o alle Regioni, in ragione dela dimensione dell'emergenza.

[82] Poiché si tratta di ipotesi dalla descrizione molto generica, si suggerisce di annotare sulla cartella clinica le circostanze che hanno fatto ritenere opportuno utilizzare questa modalità. Va sottolineato che non si tratta di eccezione all'ottenimento del consenso informato ma solo di suo differimento.

- l'introduzione di barriere di cortesia e la corretta utilizzazione dei locali, che evitino l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;
- il rispetto della dignità dell'interessato in occasione della prestazione medica;
- la garanzia che possa essere data, in modo corretto, ai soli terzi legittimati, notizia o conferma anche telefonica di una prestazione di pronto soccorso[83];
- la previsione di modalità adeguate per la visita di terzi legittimati agli interessati ricoverati, rispettandone eventuali volontà contrarie;
- messa in atto di procedure finalizzate a impedire una correlazione tra interessato e reparto o struttura di ricovero e cura, che faccia comprendere lo stato di salute posseduto;
- la sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.

La mancata adozione di tali misure non è punita da una sanzione specifica, ma, dando luogo ad un trattamento di dati in violazione di quanto previsto dal Codice, potrebbe provocare una censura da parte del Garante (art. 154) oppure, se la disattenzione provoca un danno, ingenerare una responsabilità di ordine civile a carico della struttura sanitaria. (art. 15)

Art 84 Comunicazione di dati all'interessato

I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato solo per il tramite di un medico designato dall'interessato o dal titolare.
Il titolare o il responsabile possono autorizzare per iscritto gli esercenti le professioni sanitarie diversi dai medici, infermieri e personale normalmente operante in una struttura medico ospedaliera, affinché rendano noti all'interessato i propri dati inerenti la salute.
Si tratta di una vera e propria nomina ad incaricato. Il titolare designa un soggetto, che a sua volta potrà autorizzare per iscritto i soggetti indicando loro per iscritto modalità e cautele per trattare i dati e svolgere questo ruolo.

Art. 85 Compiti del Servizio sanitario nazionale

Tale articolo individua le finalità di interesse pubblico rientranti nei compiti del SSN; si tratta di tutte le attività amministrative correlate alla prevenzione, cura e riabilitazione, nonché ai trapianti di organo e di tessuto, alle trasfusioni, la programmazione e vigilanza dell'assistenza sanitaria, le attività certificatorie, l'applicazione della normativa di igiene e sicurezza sul posto di lavoro, i rapporti tra i soggetti del SSN.

Art. 86 Altre finalità di rilevante interesse pubblico

In questa categoria rientrano le attività amministrative correlate all'applicazione della disciplina in materia di tutela della maternità e interruzione volontaria della gravidanza,

[83] La disciplina di legge prevede che questi casi siano regolamentati e non autorizza la non comunicazione. Ad es. se un padre cerca il proprio congiunto al P.S. la notizia va fornita mentre se la richiesta viene fatta da un giornalista allora saranno adottate delle precauzioni.

stupefacenti e sostanze psicotrope, assistenza, integrazione sociale e diritti delle persone handicappate.

Artt. 87, 88 e 89 — Le prescrizioni mediche: medicinali a carico e non del SSN e casi particolari

Il codice distingue tra medicinali a carico, oppure no, del Servizio Sanitario Nazionale.

1. Nel primo caso le ricette sono redatte secondo un modello che consente di risalire all'identità dell'interessato solo in caso di necessità, connesse al controllo della correttezza della prescrizione, a fini di verifiche amministrative, per scopi epidemiologici e di ricerca. Il modello di ricetta è predisposto al fine di potere separare la parte contenente la prescrizione da quella contenente le generalità dell'assistito.
2. Nel secondo caso, le generalità dell'interessato non sono apposte sulla ricetta, se non nel caso in cui il medico ritenga indispensabile risalire all'identità del soggetto per una effettiva necessità dello stesso.
3. Nei casi specifici collegati agli stati di tossicodipendenza, nei quali deve essere accertata l'identità dell'interessato a cui vengono somministrate specifiche sostanze, le ricette sono conservate separatamente da ogni altro documento che non ne richiede l'utilizzo.
4. A integrazione del Dlgs 539/92 in materia di medicinali per uso umano, il testo unico prevede che decorsi i sei mesi, per i quali il farmacista è tenuto a conservare le ricette mediche, qualora non le consegni all'autorità competente per il rimborso del prezzo a carico del SSN, il farmacista stesso distrugga le ricette con modalità atte a escludere l'accesso di terzi ai dati in esse contenuti.

Possono essere introdotte comunque, a integrazione di quanto stabilito, specifiche disposizioni che prevedono il rilascio di ricette non identificative dell'interessato.

Decorrerà dal 1 gennaio 2005 l'obbligo di nascondere nelle prescrizioni di medicinali le generalità del paziente.

Art. 90 — Trattamento dei dati genetici e donatori di midollo osseo

Il trattamento dei dati genetici può avvenire solo con specifica autorizzazione rilasciata dal Garante, sentito il ministro della Salute, e con parere del Consiglio superiore di sanità. Tale autorizzazione deve altresì indicare tutti gli ulteriori elementi di informativa da fornire all'interessato, in ragione della complessità del trattamento.

Il donatore di midollo osseo ha il diritto e il dovere di mantenere l'anonimato, sia nei confronti del ricevente sia nei confronti di terzi.

La legge non definisce quali siano i dati genetici[84]; inoltre, vi sono casi in cui il loro trattamento è legittimato da motivi di cura, diagnosi e prevenzione. Ci si augura, quindi, che il Garante farà pervenire una Autorizzazione generale, in via preventiva.

[84] Per una definizione di "dato genetico" possiamo rifarci alla nozione contenuta nella Raccomandazione N.R (97) 5 adottata dal Consiglio d'Europa che comprende " tutti i dati indipendentemente dalla tipologia, che riguardano i caratteri ereditari di un individuo o le modalità di trasmissione di tali caratteri nell'ambito di un gruppo di individui legati da vincoli di parentela".

Art. 91 Dati trattati mediante carte

Il trattamento di dati sensibili idonei a rivelare lo stato di salute e la vita sessuale, registrati e/o trattati mediante carte, quali la carta nazionale dei servizi, è consentito solo in virtù del principio di necessità[85] e con la adozione delle misure e degli accorgimenti a garanzia dell'interessato.

Art. 92 Cartelle cliniche

La cartella clinica deve essere conservata con i seguenti accorgimenti:

1. deve essere assicurata la comprensibilità dei dati;
2. devono essere distinti i dati del paziente da quelli eventualmente riguardanti altri interessati,compresi i nascituri;
3. eventuali richieste di presa visione o di rilascio di copia della cartella e della scheda di dimissione ospedaliera, da soggetti diversi dall'interessato, devono essere giustificate dalla necessità di far valere un diritto in sede giudiziaria o dalla necessità di tutelare una situazione giuridicamente rilevante di rango pari a quella dell'interessato o consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Art. 93 Certificato di assistenza al parto

Ai fini della dichiarazione di nascita, il certificato di assistenza al parto è sostituito da una semplice attestazione contenente i soli dati richiesti nei registri di nascita. Nel caso in cui la madre abbia richiesto di non volere essere nominata, il certificato di assistenza al parto o la cartella clinica, che rendono identificabile la stessa, possono essere rilasciati in copia integrale a chi vi abbia interesse decorsi cento anni dalla formazione del documento, ai sensi dell'art. 30, comma 1, del Dpr n. 396/2000 (l'accesso è consentito solo con le opportune cautele per evitare che la madre sia identificabile).

Art. 94 Banche di dati, registri e schedari in ambito sanitario

Anche banche dati, registri, archivi e schedari in ambito sanitario, già formati prima dell'entrata in vigore del testo unico, devono conformarsi alle disposizioni innovative previste in generale per l'accesso.

TITOLO VIII
LAVORO E PREVIDENZA SOCIALE

Capo I

[85] Si rimanda al principio generale contenuto nell'art. 3 del Codice.

Profili generali

Art. 111 Codice di deontologia e di buona condotta

In questo Titolo il codice sulla privacy raccoglie le disposizioni relative ai rapporti di lavoro e i rapporti previdenziali. Rinvia però all'iniziativa del Garante l'attivazione di "codici di deontologia e di buona condotta" che dovranno contenere le regole per il trattamento dei dati personali effettuato per finalità previdenziali o per la gestione del rapporto di lavoro, da parte di soggetti pubblici e privati.
Il codice privacy rimanda a questi codici la regolamentazione dell'informativa all'interessato e le modalità di acquisizione del consenso relativamente alla pubblicazione degli annunci per finalità di occupazione e alla ricezione di curricula contenenti dati personali anche sensibili.

Capo III
Divieto di controllo a distanza e telelavoro

Artt. 114 Controllo a distanza

Tale articolo, relativo al divieto di controllo a distanza dei lavoratori si limita a confermare le disposizioni dell'art. 4 della legge 300/1970, mantenendo quindi il divieto di usare impianti audiovisivi e altre apparecchiature per il controllo a distanza dell'attività dei lavoratori.
Qualora tali impianti fossero necessari per finalità produttive od organizzative[86] (anche di sicurezza) l'installazione può essere effettuata solo previo accordo sindacale o, in difetto, su provvedimento della Direzione Provinciale del Lavoro – Servizio Ispettivo. Occorre che i dipendenti siano informati in maniera chiara ed esatta circa le modalità utilizzate dal datore nell'effettuare i controlli[87].

[86] Il Garante ha indicato con Provvedimento generale del 29 novembre 2000 le garanzie con le quali le installazioni di impianti di video sorveglianza sono consentite: 1. tutti gli interessati devono determinare esattamente le finalità perseguite attraverso la video sorveglianza e verificarne la liceità in base alle norme vigenti; 2. il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi; 3. nei casi in cui la legge impone la notificazione al Garante dei trattamenti dei dati personali effettuati da determinati soggetti, questi devono indicare fra le modalità di trattamento anche la raccolta di informazioni mediante apparecchiature di video sorveglianza. 4. si devono fornire alle persone che possono essere riprese indicazioni chiare che avvertano della presenza di impianti di video sorveglianza; 5. occorre rispettare il divieto di controllo a distanza del lavoratore; 6. occorre rispettare i principi di pertinenza e di non eccedenza; 7. occorre determinare con precisione il periodo di conservazione delle immagini, 8. occorre designare, per iscritto, i soggetti –responsabili e incaricati del trattamento dei dati – che possono utilizzare gli impianti e prendere visione delle registrazioni; 9. i dati raccolti per determinati fini (ad es, per ragioni di sicurezza o di tutela del patrimonio) non possono essere utilizzati per finalità diverse; 10. gli impianti per la rilevazione degli accessi dei veicoli ai centri storici devono essere conformi anche alle diposizioni contenute nel D.P.R.n. 250/99.
[87] La Azienda USL di Pescara ha adottato un "Regolamento per l'utilizzo degli impianti di video sorveglianza ai fini di sicurezza, tutela del patrimonio, controllo degli accessi e

ART. 115 Telelavoro e lavoro a domicilio

La riservatezza deve essere assicurata dal datore di lavoro, anche nei rapporti di lavoro a domicilio o domestico.

TITOLO X
COMUNICAZIONI ELETTRONICHE

Capo I
Servizi di comunicazione elettronica

Il Codice ha recepito i contenuti della direttiva n. 2002/58/CE: dalla constatazione della crescente convergenza fra i settori delle telecomunicazioni, dei media e delle tecnologie dell'informazione, il legislatore comunitario ha voluto assoggettare tutte le reti di trasmissione e i servizi correlati a un unico quadro normativo. Si è voluto prescindere dal fatto che i dati personali siano utilizzati sulle reti telefoniche o sul web.
In quest'ottica è stata emanata una "direttiva quadro" (2002/21/Ce) che ha istituito la cornice normativa comune per le reti e i servizi di comunicazione elettronica, e quattro "direttive particolari". Alla direttiva n. 58, si aggiungono quella relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica (2002/20/CE); quella sull'accesso alle reti di comunicazione elettronica e alle risorse correlate nonché all'interconnessione delle stesse (2002/19/CE); e quella sul servizio universale e sui diritti degli utenti in materia di reti e servizi di comunicazione elettronica (2002/22/CE).
Che il codice della privacy dovesse porre ordine e disciplina anche nel trattamento dei dati personali connesso alla fornitura di servizi di c.d. comunicazione elettronica era ovvio, così come ovvia era l'attesa di regole capaci di coniugare la tutela costituzionale della libertà e segretezza delle comunicazioni con le esigenze del procedimento penale, dove l'impiego di quei dati, a fini di indagine e prova, si è fatta progressivamente più utile e necessaria.

Art. 132 Conservazione di dati di traffico per altre finalità

Il quadro regolamentare delineato dalle recenti modifiche apportate dal decreto legge 354/03, convertito con modificazioni dalla legge 45/2004, all'articolo 132 del Codice non è particolarmente felice dal punto di vista investigativo sia per quanto riguarda la durata della conservazione dei dati che per le modalità.
Esso si contraddistingue per questi peculiari e significativi aspetti:

a) la conservazione prolungata dei dati, ai fini del procedimento penale, è stabilita con riguardo al solo traffico telefonico, con esclusione, quindi, in particolare dei dati internet;

---

monitoraggio continuo dei pazienti ricoverati nei reparti ove presenti tali impianti, per il trattamento dei dati personali.

b) i tempi di conservazione del periodo base e del periodo "ulteriore" è presupposto legittimante l'acquisizione la sussistenza di sufficienti indizi di colpevolezza di uno dei citati gravi delitti;
c) per l'accesso e l'acquisizione dei dati è necessario in ogni caso un decreto motivato del giudice (su richiesta del P.M. o di un difensore); per il periodo "ulteriore" è presupposto legittimante l'acquisizione la sussistenza di sufficienti indizi di colpevolezza di uno dei citati gravi delitti;[88]
d) il difensore può richiedere direttamente la documentazione al fornitore del servizio, ai sensi dell'art. 391-quater del C.P.P., dei soli dati relativi alle utenze del proprio assistito, ivi compresi, quelli relativi al traffico in entrata, quando dall'omissione può derivare effettivo e concreto pregiudizio per lo svolgimento delle investigazioni difensive;
e) il trattamento dei dati è effettuato con il rispetto delle misure previste dal codice, art. 17, per i trattamenti che presentano "rischi specifici per i diritti e le libertà fondamentali" e stabiliti dal Garante nell'ambito di una verifica all'inizio del trattamento.

L'obbligo di conservazione dei dati è soggetto a un regime differenziato a seconda che si tratti di dati inerenti il solo traffico telefonico oppure il traffico di tutti gli altri mezzi di comunicazione elettronica.

Riguardo ai dati telefonici, la legge 45 ha ristretto sia l'ambito di applicazione di conservazione dei dati al solo traffico telefonico, sia la durata di conservazione, stabilita in 24 mesi per finalità di accertamento e repressione dei reati. L'acquisizione dei dati presso il fornitore avviene ora anche entro i primi 24 mesi esclusivamente dietro decreto motivato del giudice su istanza del pubblico ministero. Scaduto il primo termine di 24 mesi il giudice autorizza l'acquisizione dei dati, con decreto motivato, per ulteriori 24 mesi[89] se ritiene sussistano sufficienti indizi dei delitti di cui all'art. 407, comma 2, lett. a) del C.P.P[90] Fino alla data in cui diverranno efficaci le misure e gli accorgimenti prescritti dal Garante per la conservazione del traffico telefonico si osserva il termine di 5 anni.

I dati in rete. La disciplina inerente la conservazione e acquisizione dei dati di traffico di tutti gli altri mezzi di comunicazione elettronica, Internet e posta elettronica inclusi, prevede un obbligo di conservazione ordinario dei dati relativi al solo traffico di soli 6 mesi.

Capo III
Video sorveglianza

Art. 134 Codice di deontologia e di buona condotta

[88] Delitti di cui all'art. 407, comma 2, lett. a): strage, terrorismo, associazione per delinquere, omicidio, sfruttamento della pornografia minorile, ecc., del C.P.P., nonché dei delitti in danno di sistemi informatici o telematici.

[89] Resta da stabilire se i dati del traffico telefonico, il cui accesso resta precluso dopo la scadenza dei termini sopra indicati, possano ugualmente essere utilizzati come prova se acquisiti prima dell'entrata in vigore dell'attuale legge e se possano essere acquisiti anche successivamente, con strumenti alternativi, attraverso le scritture contabili e di fatturazione che le società sono tenute a conservare per tempi molto più lunghi per dimostrare l'osservanza delle normative fiscali.

Tale articolo prevede che la materia sia oggetto di disciplina per mezzo di un codice per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini. Nelle more delle definizione di tale codice si fa riferimento ad un Provvedimento emanato dal Garante il 29 novembre 2000 "Decalogo per la video sorveglianza".

PARTE III
TUTELA DELL'INTERESSATO E SANZIONI

Art. 141 Forme di tutela

Gli articoli dal 141 al 151 disciplinano le forme di tutela azionabili di fronte al Garante, contro i trattamenti illeciti di dati personali effettuati da chiunque gestisca banche dati di qualsiasi tipo. Le azioni esperibili sono il reclamo, la segnalazione e il ricorso, che vanno indirizzate al Garante senza particolari formalità, allegando gli eventuali documenti utili.
Il Codice ha introdotto una distinzione tra una forma amministrativa di intervento del Garante, posto in essere allo scopo di reprimere le violazioni della normativa, ed il procedimento che innanzi allo stesso viene attivato per garantire i diritti dell'interessato.
L'art. 141 prevede che il procedimento amministrativo possa essere attivato a seguito di un "reclamo circostanziato[91]" o di una "segnalazione[92]" dell'interessato.

Art. 142 Proposizione dei reclami

Il reclamo al Garante è proponibile per rappresentare, con dati circostanziati, una qualsiasi violazione della disciplina rilevante in materia di trattamento di dati personali. Al reclamo corrisponde un dovere di pronuncia del Garante. Mediante il reclamo può chiedersi tutela in presenza di una qualsivoglia violazione della disciplina rilevante in materia di trattamento di dati personali. Il reclamo, dunque, è esperibile in presenza della violazione di disposizioni che incidano sul trattamento dei dati personali.
Il reclamo può essere proposto dall'interessato personalmente, sottoscrivendo il relativo atto o da associazioni che lo rappresentino.
Si chiede al reclamante di indicare un recapito per l'invio di comunicazioni anche tramite posta elettronica, fax o telefono.

Art. 143 Procedimento per i reclami

[91] Deve contenere un'esposizione dettagliata dei fatti e delle norme violate.
[92] Ha carattere generico e presuppone un'indagine più approfondita da parte del Garante per verificare la sussistenza dei fatti segnalati.

L'attività istruttoria[93] non è stata specificata e si deve pertanto ritenere che la stessa debba essere definita attraverso un giusto equilibrio tra poteri e doveri istruttori delle parti e compiti del Garante.
Sono invece indicati i provvedimenti che il Garante può assumere:

- invitare il titolare, anche con contraddittorio con l'interessato, a effettuare il blocco spontaneo, prima di prescrivere al titolare le misure di cui alla lettera b) dell'art.143;
- prescrivere al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti;
- può disporre il divieto o il blocco, in tutto o in parte, del trattamento che risulta illecito o non corretto;
- vietare in tutto o in parte il trattamento dei dati relativi a singoli soggetti o a categorie di soggetti che si pone in contrasto con rilevanti interessi della collettività[94]. Si tratta di misure che, possono essere assunte anche in via cautelare, alla luce di una cognizione sommaria che si avvale di una istruttoria preliminare che porti a ritenere che il reclamo non è manifestamente infondato.

E' prevista una particolare forma di notificazione disposta dal Garante, mediante pubblicazione sulla Gazzetta Ufficiale, nel caso in cui i destinatari non siano facilmente identificabili.
Contro i provvedimenti emessi dal Garante ai sensi dell'art. 143 è ammesso ricorso all'autorità giudiziaria ex art. 152. Il ricorso deve essere proposto entro il termine di 30 giorni dalla data di comunicazione del provvedimento o dalla data di rigetto tacito.
Se il ricorso viene proposto oltre tale termine il giudice lo dichiara inammissibile con ordinanza che è ricorribile in Cassazione.

Art. 144 Segnalazioni

Si tratta di comunicazioni informali e non circostanziate al Garante, con cui l'interessato sollecita un controllo da parte di quest'ultimo sulle prospettate violazioni della disciplina in materia di trattamento dei dati personali. Il Garante in esito alla istruttoria compiuta potrà adottare, anche in via cautelare, i provvedimenti con cui può essere definito il procedimento di reclamo.
Il richiamo operato dall'art. 152 ai provvedimenti ex articolo 143, e, a sua volta, il richiamo effettuato nell'articolo 144 e nell'art. 143, inducono a ritenere che anche i provvedimenti emessi in esito alle segnalazioni siano ricorribili dinanzi all'autorità giudiziaria.

Art. 145 Ricorsi

Il ricorso è una tutela per via amministrativa alternativa a quella giurisdizionale. Tale articolo, infatti, stabilisce come il ricorso al Garante non possa essere proposto se, per il medesimo oggetto e tra le stesse parti, è già stata adita l'autorità giudiziaria. Così come il ricorso al

[93] Non si può escludere che il procedimento di che trattasi possa essere attivato anche d'ufficio. Siamo infatti in presenza di attività amministrativa volta alla repressione di illeciti, per il cui espletamento l'Amministrazione competente può attivarsi autonomamente.
[94] La mancata ottemperanza a questa disposizione non è però sanzionata penalmente, poiché l'art. 170 del Codice si riferisce solo ai provvedimenti emanati dal Garante ai sensi dell'art. 143, comma 1, lett. C). ne consegue che tutte le altre disposizioni emanate ai sensi del medesimo articolo non sono munite di sanzione penale.

Garante rende improponibile un'ulteriore domanda all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto.

Art. 146 Interpello preventivo

Il legislatore ha fissato una condizione di procedibilità – interpello preventivo – per la proposizione del ricorso al Garante, derogabile solo in caso di urgenza, in presenza di un pregiudizio imminente e irreparabile. L'interessato, pertanto, per potere esperire il ricorso al Garante deve presentare la domanda che costituirebbe oggetto del ricorso al titolare o al responsabile. Solo dopo il termine di 15 giorni dalla ricezione della domanda, o in casi particolari di 30 giorni, o qualora sia stato opposto alla richiesta un diniego anche parziale, può esperirsi il ricorso.
L'interessato può tuttavia agire direttamente, senza rispettare tale termine dilatorio, se sussiste un'urgenza di provvedere dettata dal pericolo di subire un danno imminente ed irreparabile.

Art. 147 Presentazione del ricorso

Tale articolo specifica il contenuto e le modalità di presentazione del ricorso nei confronti del titolare. Vanno indicate: le parti, il domicilio eletto, l'esperimento dell'interpello preventivo, le ragioni della domanda e i provvedimenti richiesti. Il ricorso oltre che dall'interessato può essere proposto dal procuratore speciale. La sottoscrizione del ricorso deve essere autenticata, a meno che sia stata apposta presso l'ufficio del Garante, o con firma digitale, o il procuratore speciale sia un avvocato cui è stata conferita procura alle liti.
Il ricorso oltre a essere presentato al Garante, può essere trasmesso con plico raccomandato o per via telematica.

Art. 148 Inammissibilità del ricorso

Tra le ragioni di inammissibilità del ricorso ci sono: la mancanza di legittimazione attiva del ricorrente, il mancato esperimento dell'interpello preventivo, la pendenza di analoga controversia dinanzi all'autorità giudiziaria.
E' previsto, a pena di inammissibilità, che il ricorso che risulti carente di alcuni degli elementi indicati dall'art. 147, commi 1 e 2, possa essere integrato dal ricorrente o di propria iniziativa, entro sette giorni dalla presentazione o su sollecitazione del Garante entro sette giorni dalla ricezione dell'invito.

Art. 149 Procedimento relativo al ricorso

Il procedimento, che deve svolgersi nel termine di 60 giorni, prorogabile se gli accertamenti sono particolarmente complessi o vi è l'assenso delle parti per ulteriori 40 giorni, si articola nel seguente modo:

- verifica dell'ammissibilità e della non manifesta infondatezza del ricorso;
- eventuale invito alla regolarizzazione;
- comunicazione del ricorso al titolare a cura del Garante con invito all'adesione spontanea, che, se accolto, determina il non luogo a provvedere sul ricorso;

- contestuale comunicazione al ricorrente e al titolare del termine per il deposito di memorie e documenti e della data in cui le parti possono essere sentite in contraddittorio;
- espletamento anche d'ufficio di una o più perizie.

Nel corso del procedimento il titolare, anche alla luce delle eccezioni della controparte, può precisare la domanda.

Art. 150 Provvedimenti a seguito del ricorso

Tale articolo distingue le misure cautelari dai provvedimenti che possono essere assunti nel giudizio. In via cautelare il Garante può disporre in via provvisoria il blocco in tutto o in parte di taluno dei dati, o l'immediata sospensione di una o più operazioni di trattamento. La misura decade se non viene definito nei termini il procedimento ed è impugnabile insieme alla decisione del ricorso. Con la pronuncia finale il Garante in sede di accoglimento del ricorso ordina al titolare la cessazione del comportamento illegittimo indicando le misure necessarie a tutela dei diritti dell'interessato e dando un termine per l'adozione. La mancata adozione delle misure prescritte dal Garante è sanzionata penalmente (art. 170 che prevede, fra l'altro, come chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi dell'art. 150, commi 1 e 2, e 143 comma 1, lettera c), è punito con la reclusione da tre mesi a due anni).
Il garante previa richiesta delle parti statuisce sulle spese e sui diritti relativi al ricorso, che possono essere poste a carico del soccombente o compensate per giusti motivi. Se non vi è opposizione la pronuncia sulle spese costituisce titolo esecutivo.
La mancata osservanza ai provvedimenti, sia interinali sia definitivi, emanati dal garante è sanzionata penalmente con la reclusione.[95]
Il provvedimento finale, una volta divenuto definitivo per mancata opposizione, costituisce titolo esecutivo per la riscossione forzata delle spese.

Art. 151 Opposizione

I provvedimenti assunti dal Garante in esito al ricorso o il rigetto tacito possono essere opposti dinanzi al tribunale con il ricorso disciplinato dall'art. 152, che investirà l'autorità giudiziaria della questione sostanziale già oggetto di pronuncia del Garante. La proposizione del ricorso non sospende automaticamente l'efficacia del provvedimento del Garante[96].

Art. 152 Attività giudiziaria ordinaria

Il giudice ordinario, tribunale in composizione monocratica, è competente a decidere delle controversie in ordine all'applicazione delle disposizioni del codice sulla privacy e a quelle relative ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione. Il provvedimento del Garante assunto in sede di reclamo è ricorribile al tribunale così come il provvedimento ex art. 152,comma 2, è opponibile dinanzi al tribunale.
Il termine per la presentazione del ricorso all'autorità giudiziaria avente a oggetto un

[95] Si rimanda all'art. 170 del Codice.
[96] Il Garante si pone in una posizione di terzietà di fronte ad una controversia di parti.

provvedimento del Garante è di 30 giorni dalla comunicazione (anche per via fax o posta elettronica) del provvedimento o dalla data del rigetto tacito.
Il legislatore ha attribuito al G.O. il potere di annullare i provvedimenti delle P.A. contrastanti con il Codice, ove richiesto dal ricorrente. Il comma 12 dell'articolo riferisce infatti il potere del G.O. di derogare al divieto di annullamento degli atti amministrativi anche "all'eventuale atto del soggetto pubblico titolare o responsabile" del trattamento dei dati in questione.
Va evidenziato che la giurisdizione ordinaria esclusiva non comprende solo le controversie per l'applicazione dei diritti dell'interessato di cui all'art. 7 del Codice ma anche ogni altra lite.
La competenza territoriale p. 145

TITOLO II
L'AUTORITA'

Capo I
Il Garante per la protezione dei dati personali

Art. 153 Il Garante

Trattasi di una autorità autonoma e indipendente[97] di controllo che mantiene la forma di organo collegiale composto da quattro membri eletti dalle assemblee parlamentari – nominati due dalla Camera dei deputati e due dal Senato -, i quali eleggono il presidente al loro interno – le decisioni del Garante sono prese a maggioranza, ma in caso di parità di voti, il voto del presidente prevale – e rimangono in carica per quattro anni, potendo essere confermati soltanto una volta.

Art. 154 Compiti

In relazione ai compiti del Garante la elencazione di cui al primo comma è stata distinta dalle funzioni di controllo o assistenza attribuite al Garante, sempre per la specifica materia della tutela dei dati personali, con riferimento ad un'aggiornata serie di leggi di ratifica di accordi o convenzioni internazionali o ai regolamenti comunitari che le prevedono
Rimango attribuite al Garante, quale autorità designata ai fini della cooperazione tra Stati in base alla Convenzione n. 108 del Consiglio d'Europa, per quanto concerne l'attività di assistenza sulla protezione delle persone rispetto al trattamento automatizzato dei loro dati.

[97] Le Autorità Indipendenti sono soggetti dotati di ampia autonomia e deputati a svolgere funzioni di regolamentazione in ambiti della vita sociale ove il contemperamento degli interessi contrapposti si presenta particolarmente difficile e delicato. La funzione tutoria delle Autorità si distingue da quella di amministrazione attiva e si sostanzia in poteri di indirizzo e di controllo. La funzione tutoria consiste nel tutelare il diritto delle persone sulle informazioni che direttamente la riguardano, in particolare per quanto attiene al diritto alla riservatezza e all'identità personale.
L'autonomia delle Autorità Indipendenti si sostanzia nella facoltà di darsi le regole per il funzionamento dei propri organi ed in quella di articolare e modificare le proprie piante organiche.

Sintetizzando, i compiti che il Garante può svolgere anche avvalendosi dell'ufficio sono:

- controllare se i trattamenti sono effettuati nel rispetto della normativa vigente e in conformità alla notificazione, anche dopo la cessazione del trattamento;
- esaminare le istanze di tutela amministrativa, ossia reclami, segnalazioni e ricorsi, presentate dagli interessati o dalle associazioni che li rappresentano;
- impartire ai titolari del trattamento le prescrizioni sulle misure necessarie o opportune per rendere il trattamento dei dati conforme alla legge;
- vietare, anche parzialmente, il trattamento illecito o non corretto dei dati o disporne il blocco qualora, data la natura dei dati o delle modalità del trattamento o degli effetti che questo può determinare, ci sia il rischio che uno o più interessati vengano danneggiati;
- promuovere la sottoscrizione di codici di deontologia per particolari settori o materie;
- segnalare anche al parlamento, e non solo al Governo, l'opportunità di interventi normativi anche a seguito dell'evoluzione del settore, con l'ulteriore precisazione però che tale segnalazione è effettuata dall'Autorità per la necessità di tutelare i diritti fondamentali della persona;
- esprimere pareri nei casi previsti;
- promuovere e dare ampia conoscenza tra il pubblico delle norme che regolano la materia (in particolare delle misure di sicurezza);
- denunciare i fatti che possono essere configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle sue funzioni;
- tenere il registro dei trattamenti dei dati personali effettuati da soggetti pubblici e privati, formatosi sulla base delle notificazioni ricevute secondo il nuovo sistema previsto dal codice;
- predisporre ogni anno una relazione sull'attività svolta e sullo stato di attuazione del codice, da trasmettere al Parlamento e al Governo entro il 30 aprile dell'anno successivo.

Nell'ambito degli ulteriori compiti affidati al Garante si evidenzia che nell'ambito della consultazione obbligatoria prevista per gli schemi di norme regolamentari e atti amministrativi di provenienza ministeriale che incidono su materie di propria competenza, l'Autorità deve adottare il parere,- salvi i termini più brevi previsti – entro 45 giorni dal ricevimento della richiesta. Decorso tale termine l'amministrazione richiedente potrà procedere indipendentemente dall'acquisizione del parere.

Capo II
L'Ufficio del Garante

Art. 155 Principi applicabili
Art. 156 Ruolo organico e personale

L'Ufficio posto alle dipendenze del Garante, a cui è preposto un segretario generale, si compone di un contigente organico di 100 unità di personale dipendente. Vengono opportunamente precisate, in armonia con le norme sul segreto d'ufficio del cp (art. 326), le disposizioni sugli obblighi del medesimo personale e di eventuali consulenti dell'Autorità alla segretezza e alla riservatezza delle informazioni di cui vengono a conoscenza, nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete.

Capo III
Accertamenti e controlli

Riguardo al capo III, interamente dedicato ai poteri di accertamento e controllo attribuiti al Garante, va rimarcata la differenza di questo codice che, a differenza dei precedenti testi unici c.d. "misti", ha riunito e assorbito in una unica disciplina le previdenti norme della legge n. 675/96 e quelle regolamentari di esecuzione o attuazione del dettato legislativo, attribuendo a queste ultime direttamente e senza particolari rielaborazioni un rango primario.

Art. 157 Richiesta di informazioni e di esibizione di documenti

Il garante, nell'espletamento della sua attività ispettiva e di controllo, puòà chiedere al titolare, al responsabile, all'interessato e a terzi di "fornire informazioni e di esibire documenti".

Art. 158 Accertamenti

Nell'espletamento degli accertamenti il Garante si avvale, oltre che del proprio personale, "della collaborazione di altri organi dello Stato". L'articolo in questione regolamenta le modalità che regolano l'accesso presso "un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze".

Art. 159 Modalità

Rimane il potere del Garante di richiedere informazioni o l'esibizione di documenti nonché di disporre sia l'accesso a banche-dati o archivi, sia le ispezioni e le verifiche nei luoghi ove si svolgono i trattamenti dei dati personali (avvalendosi, ove necessario, della collaborazione di altri organi dello Stato, come, ad es., la Guardia di Finanza con cui l'Autorità ha siglato un apposito protocollo d'intesa nel 2002.)
In questo secondo caso, se gli accertamenti sono svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze sono però necessari l'assenso informato del titolare o del responsabile del trattamento oppure l'autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dove avviene l'accertamento.
E' stata inoltre ripresa la previsione secondo cui il provvedimento conclusivo del Garante relativo anche alle spese eventualmente sostenute per svolgere gli accertamenti, senza la collaborazione dei soggetti sottoposti al procedimento di controllo, costituisce titolo esecutivo ai sensi del codice di procedura civile.

Art. 160 Particolari accertamenti

Con riferimento a taluni trattamenti svolti da parte delle forze dell'ordine, o comunque da autorità o organi pubblici in ambito giudiziario, e per finalità di difesa e sicurezza dello Stato, la loro esecuzione può essere affidata unicamente a un componente designato dal Garante.
Per consentire il corretto svolgimento delle attività di uffici giudiziari, sono stati poi introdotte alcune cautele consistenti nell'adozione di idonee modalità di controllo che tengano conto anche della particolare collocazione istituzionale dell'organo interessato e della necessità, quando vi sia richiesta dell'organo procedente, di differire gli accertamenti nel caso gli atti d'indagine siano coperti dal segreto.
In tale ambito, è stata infine inserita un'ulteriore disposizione che sembra rivestire carattere più generale e non riferirsi al solo profilo delle risultanze delle specifiche attività di controllo del Garante svolte nei confronti di uffici giudiziari, riguardando la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento, che restano comunque disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale.

TITOLO III
SANZIONI

Capo I
Violazioni amministrative

Il Titolo III del codice della privacy è espressamente dedicato alle sanzioni distinguendo tra violazioni amministrative[98] e illeciti penali.
Attraverso le violazioni amministrative il Legislatore tende a sanzionare una serie di comportamenti illeciti, sia nei confronti degli interessati, sia nei confronti del Garante.

Art. 161 Omessa o inidonea informativa all'interessato

Le violazioni amministrative consistono in:

1. omessa o inidonea informativa all'interessato[99]. Verificandosi questa violazione viene punito:

[98] Il Codice, all'art. 166, richiama esplicitamente l'applicazione delle norme generali in materia stabilite dalla L.n. 689/1981. anzitutto, il **principio di legalità** in forza del quale la comminatoria di sanzioni deve essere prevista in un atto avente forza di legge. L'**elemento soggettivo dell'illecito amministrativo** è costituito dal dolo o dalla colpa: la sanzione può essere irrogata se sussiste almeno quest'ultima in capo all'agente. Non è punibile chi ha compiuto il fatto. La responsabilità è esclusa quando sussiste una **causa legittima di giustificazione**, cioè: adempimento del dovere, stato di necessità, legittima difesa. Se la violazione è compiuta dal rappresentante o da un dipendente di una persona giuridica, quest'ultima è obbligata in solido con l'autore al pagamento della sanzione, con possibilità di regresso.

[99] Riguarda oltre che il Responsabile, anche gli Incaricati del trattamento. Sarà soggetto alla sanzione il Responsabile del trattamento se non ha disposto le opportune misure organizzative

a. con la sanzione amministrativa pecuniaria del pagamento di una somma da 3 mila a 18 mila euro, la violazione degli obblighi di informativa all'interessato circa i dati, previsti dall'art. 13 ("finalità e modalità del trattamento, natura obbligatoria o facoltativa del loro conferimento, termini di una ulteriore comunicazione dei dati, ecc.").
b. con il pagamento di una somma da 5 mila a 30 mila euro, nel caso in cui la medesima violazione riguardi dati sensibili o giudiziari, o dati che presentino, ai sensi dell'art. 17, rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

L'art. 161 prevede, altresì che, in ambedue le ipotesi, "la somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore".

Art. 162 Altre fattispecie

Tale articolo prevede ipotesi sanzionatorie diverse:

- nel comma 1, fissa la sanzione del pagamento di una somma da 5 mila a 30 mila euro, in due ipotesi: nel caso in cui la cessione dei dati avvenga in violazione di quanto previsto dall'art. 16, comma 1, lett. B) – cioè quando i dati vengono ceduti ad altro titolare, purchè destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti -; nel caso in cui la cessione avvenga in violazione di altre disposizioni relative alla disciplina del trattamento dei dati medesimi.
- Nel comma 2, prevede la sanzione del pagamento di una somma da 500 a 3 mila euro, nel caso in cui vengano resi noti all'interessato o agli altri soggetti che, in determinate condizioni, possono riceverli in sua vece, dati idonei a rivelare lo stato di salute, facendo ciò non per il tramite di un medico designato dallo stesso interessato o dal titolare del trattamento.

Per potersi applicare la sanzione è necessario che tale modalità di comunicazione non afferisca alla comunicazione di dati forniti in precedenza dallo stesso interessato. Inoltre, è consentita l'individuazione da parte del titolare di soggetti esercenti professioni sanitarie diversi dai medici, abilitati a fornire le predette comunicazioni.

Art. 163 Omessa o incompleta notificazione

Chiunque, essendovi tenuto, non provvede tempestivamente alle notificazioni di cui agli artt. 37 e 38, ovvero indica in tali comunicazioni notizie incomplete[100], è soggetto ad una sanzione amministrativa del pagamento di una somma da 10 mila a 60 mila euro, oltre che alla pubblicazione dell'ordinanza ingiunzione, per intero o per estratto, su uno o più quotidiani.

Art. 164 Omessa informazione o esibizione al Garante

(istruzioni agli Incaricati, predisposizione della modulistica necessaria, ecc.); l'Incaricato laddove abbia omesso di dare attuazione a quanto indicato dal responsabile.

[100] Per perfezionare l'**elemento soggettivo** dell'illecito è sufficiente la colpa del soggetto agente.

E' prevista la sanzione amministrativa del pagamento di una somma da 4 mila a 24 mila euro, nei confronti di chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante.

Art. 165 Pubblicazione del provvedimento del Garante

Tra le sanzioni amministrative accessorie è prevista la pubblicazione dell'ordinanza-ingiunzione che è sempre comminata nel caso di omessa o incompleta notificazione al Garante, mentre costituisce sanzione facoltativa nel caso di irrogazione delle altre sanzioni amministrative pecuniarie previste dal capo I.

Art. 166 Procedimento di applicazione

Il Garante costituisce l'organo competente a ricevere il rapporto e a irrogare le sanzioni previste, osservandosi, in quanto compatibili, le disposizioni della legge 689/1981, in tema di sanzioni amministrative.

Capo II
Gli illeciti penali

Con gli articoli da 167 a 172 il legislatore prevede gli illeciti penali, distinguibili in delitti e contravvenzioni.

Art. 167 Trattamento illecito dei dati[101]

Il trattamento[102] dei dati personali in violazione degli articoli:

- 18[103] (trattamenti effettuati da soggetti pubblici), 19[104] (trattamenti di dati diversi da quelli sensibili e giudiziari), 23 (consenso dell'interessato per il trattamento dei dati

[101] Se il fatto integra la previsione contenuta in una norma penale che prevede un reato più grave, si applica solo la pena stabilita per quest'ultimo, ed è quindi escluso il concorso di reati.

[102] Ratio del Codice non è solo quella di approntare una tutela risarcitoria per le lesioni già prodotte ma anche di evitare che esse si verifichino.

[103] La violazione dell'art. 18 si verifica laddove venga svolto un trattamento di dati personali non necessario al raggiungimento di obiettivi di pubblico interesse o quando, pur nell'ambito del perseguimento di funzioni istituzionali dell'Ente, non siano rispettati i limiti previsti da atti normativi per il trattamento medesimo.

[104] Il reato di cui all'art. 19 si compie allorché vengono comunicati ad Enti pubblici dati personali comuni al di fuori dei casi previsti da norme di legge o di regolamento o senza che la comunicazione stessa sia necessaria per lo svolgimento delle funzioni istituzionali proprie dell'Ente. In caso di assenza di norme di legge o di regolamento, prima di iniziare la comunicazione dei dati occorre effettuare l'apposita comunicazione al Garante. L'articolo in esame richiede sotto il profilo soggettivo, non il semplice **dolo generico,** il **dolo specifico**

da parte di soggetti privati ed enti pubblici economici), 123 (dati relativi al traffico trattati dal fornitore di una rete pubblica di comunicazione), 126 (dati relativi all'ubicazione dell'utente di una rete di comunicazione), 130 (comunicazioni indesiderate) o nell'applicazione dell'art. 129 (elenchi abbonati);

- è punito con la reclusione sino a due anni, qualora il fatto sia commesso al fine di trarne profitto o di recare ad altri un danno, e sempre che dal fatto stessi derivi nocumento;
- è punito con la reclusione da sei mesi a tre anni, se il fatto, commesso con le predette finalità, consiste nella comunicazione o diffusione dei dati.

Il comma 2 dell'art. 167 prevede la pena della reclusione da uno a quattro anni, nel caso in cui taluno, al fine di trarne profitto o di recare ad altri un danno, e sempre che ne derivi nocumento, proceda al trattamento dei dati in violazione di quanto previsto da una pluralità di disposizioni espressamente indicate, tra le quali quelle relative ai dati sensibili (art. 20), ai dati giudiziari (art. 21[105]), ai dati relativi allo stato di salute (art. 22, comma 8[106]).

Art. 168 Falsità nelle dichiarazioni e notificazioni al Garante

Tale articolo punisce con la reclusione da 6 mesi a 3 anni, salvo che il fatto costituisca più grave reato, colui che dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi:

- nella notificazione del trattamento dei dati, art. 37;
- in comunicazioni, atti, documenti o dichiarazioni rese o esibiti in un procedimento innanzi al Garante;
- nel corso di accertamenti.

Tale reato di falso[107] è punito più severamente del delitto previsto dall'art. 483 del C.p. ("falsità ideologica commessa dal privato in atto pubblico") per il quale è prevista la pena della reclusione fino a due anni.
La pena prevista dall'art. 168 è più grave anche di quella generalmente prevista per le dichiarazioni false dall'art. 21 della legge 241/90.

---

consistente nell'intenzione di fare conseguire al fatto di reato un profitto, per sé od altri, o un danno a terzi. La condanna per tale reato potrà essere inflitta solo ove si dimostri che il soggetto agente: **a.** sia consapevole di avere travalicato le funzioni istituzionali dell'Ente nel trattamento dei dati; **b**.agisca con la precisa intenzione di ricavare un profitto o cagionare un danno a terzi. Se manca uno di questi elementi il fatto potrà rilevare solo sotto il profilo civilistico. Così come, la semplice colpa dell'agente, derivante da negligenza, imperizia o imprudenza, non avrà rilievo sotto il profilo penale. Va rilevato che il Codice ha subordinato la punibilità di questi reati al verificarsi di un danno.

[105] Trattamento di dati giudiziari in assenza di una norma, legislativa o regolamentare o di un provvedimento del Garante che lo autorizzi.

[106] Diffusione di dati sensibili relativi allo stato di salute.

[107] Il reato può essere compiuto da chiunque, non è quindi un reato proprio, anche se i soggetti più esposti sono i Responsabili del trattamento dei dati. L'**elemento soggettivo del reato** richiede la consapevolezza dello svolgimento di dette procedure e la consapevolezza della falsità nella dichiarazione, nell'attestazione, nell'atto o nel documento prodotto od esibito.

Art. 169 Misure di sicurezza

Si stabilisce che chi essendovi tenuto omette di adottare le misure minime di sicurezza[108], previste dall'art. 33, è punito con l'arresto sino a due anni o con l'ammenda da diecimila a cinquantamila euro.
Il legislatore, però, ha deciso di non infierire su chi omette di adottare le misure minime di sicurezza, offrendogli la possibilità di un ravvedimento operoso – entro un termine non superiore a mesi sei – e con il pagamento di una ammenda pari a un quarto di quella comminatagli.

Art. 170 Inosservanza di provvedimenti del Garante

E' prevista la pena[109] della reclusione da 3 mesi a 2 anni per chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante:

a) per il trattamento dei dati sensibili (art. 26, comma 2);
b) per il trattamento dei dati genetici e dei donatori di midollo osseo (art. 90);
c) all'esito del procedimento amministrativo di controllo svolto dal Garante sull'osservanza delle disposizioni del Codice (art. 143);
d) a seguito di ricorso, in via interdittiva o definitiva (art. 150);
e) i reati contravvenzionali.

Art. 171 Altre fattispecie

Tale articolo prevede la pena dell'ammenda da 154 a 1.549 euro e l'arresto da 15 giorni a un anno bei casi di cui agli articoli 113, comma 1, - indagini sulle opinioni dei lavoratori – e 114 – controllo a distanza –.

Art. 172 Pene accessorie

Ai sensi dell'art. 172, solo la condanna per i delitti (artt. 167, 168 e 170) comporta obbligatoriamente la pena accessoria della pubblicazione della sentenza di condanna[110].

---

[108] Il fatto di reato può essere compiuto solo da chi sia tenuto ad adottare dette misure, ciè gli Incaricati e i Responsabili del trattamento in ciascuna Amministrazione. Si tratta di un **reato proprio** perché tale qualificazione soggettiva è necessaria per integrare il fatto di reato. Il rappresentante legale del Titolare potrà essere incriminato ove non abbia provveduto a nominare alcun Responsabile: in tal caso sarà considerato Responsabile egli stesso. Il **bene giuridico tutelato** è il dato personale che viene protetto dal pericolo di perdite accidentali da parte di chi procede al trattamento. L'**elemento oggettivo del reato** consiste nella mancata adozione delle misure di sicurezza obbligatorie a prescindere dal consequenziale verificarsi di un fatto dannoso.

[109] Si tratta di un **reato doloso:** il suo perfezionamento presuppone la conoscenza del provvedimento adottato dal Garante e la volontà di non conformarsi ad esso.

[110] A norma dell'art. 36 del c.p. viene eseguita a spese del condannato in uno o più giornali indicati dal Giudice.

TITOLO IV
DISPOSIZIONI MODIFICATIVE, ABROGATIVE, TRANSITORIE E FINALI

Capo I
Disposizioni di modifica

Artt. 173 -186 L'entrata in vigore del Codice e l'incidenza sulla normativa previgente

Il Codice della privacy comporta tutta una serie di modifiche a diverse disposizioni di legge che impattano con il tema della riservatezza.
Le modifiche più sostanziali riguardano la Convenzione di applicazione dell'Accordo di Schengen, le modificazioni di atti giudiziari e le vendite giudiziarie.
Altre modifiche riguardano la Legge n. 121/1981, Nuovo ordinamento dell'Amministrazione della pubblica sicurezza; la Legge n. 241/1990, Accesso agli atti amministrativi; il D.Lgs n. 165/2001, nonché la materia della disciplina anagrafica, dello stato civile e delle liste elettorali e alcune disposizioni in materia sanitaria.
Le principali norme abrogate dalla data di entrata in vigore – 1 gennaio 2004 – del Codice sono: la Legge n. 675/96, la Legge n. 325/2000, il D.Lgs n. 282/1999; il D.P.R. n. 318/1999.
Il legislatore ha precisato che le disposizioni del Codice danno attuazione alla direttiva 96/45/Ce del Parlamento europeo e del Consiglio del 24 ottobre 1995, e alla direttiva 2002/58/Ce del parlamento europeo e del Consiglio del 12 luglio 2002.
Precisa, inoltre che, "quando leggi, regolamenti ed altre disposizioni fanno riferimento a disposizioni comprese nella legge 31.12.1996 n. 675 e in altre disposizioni abrogate dal presente codice, il riferimento si intende effettuato alle corrispondenti disposizioni del presente Codice secondo la tavola di corrispondenza riportata in allegato" e che " restano ferme le disposizioni di legge e di regolamento che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali".

Art. 177 Disciplina anagrafica, dello stato civile e delle liste elettorali

Di particolare rilevanza per il campo di nostro interesse è il comma 2 dell'articolo riguardante l'accesso del minore adottato ultraventicinquenne alle informazioni relative alla madre naturale che abbia richiesto di non essere nominata nell'atto di nascita. Con legge n. 357/74 si affermò esplicitamente che l'adottato e i genitori adottivi non potessero conoscere l'identità dei genitori naturali e tale principio fu ribadito dalle legge sulle adozioni n. 184/83, che negò il diritto dell'adottato a conoscere le proprie origini biologiche.
Con legge n. 176/91, che recepì la Convenzione internazionale dei diritti del fanciullo, si affermò che " il fanciullo è registrato immediatamente al momento della sua nascita e da allora ha diritto ad un nome, ad acquisire una cittadinanza e, nella misura del possibile, a conoscere i suoi genitori".
Tale "misura del possibile" portarono alla revisione del divieto assoluto sancito dalla legge n. 184/83 attraverso la legge n. 149/2001, nel senso che fosse consentito all'adottato, al compimento del 25° anno di età, l'accesso ai dati relativi alla propria origine in tutti i casi in cui sia stato riconosciuto alla nascita, fermo restando il divieto per coloro che non sono stati riconosciuti o qualora anche uno solo dei genitori biologici abbia dichiarato di non volere

essere nominato o abbia manifestato il consenso all'adozione a condizione di rimanere anonimo.
La norma re introdotta dal codice della privacy appare in sintonia con l'affermazione della tutela del diritto a conoscere le proprie origini, anche in quanto proclamato dalla dichiarazione dei diritti del fanciullo "nella misura del possibile".
Misura questa che trova un preciso limite nella protezione dell'anonimato della madre che non voglia essere nominata, tutelato prima e dopo l'introduzione della legge n. 184/83 al fine di impedire che le nascite non desiderate comportassero alterazioni di stato o interruzioni della gravidanza.

Art. 178 Disposizioni in materia sanitaria

In materia di Aids e infezione da Hiv sono state apportate modificazioni alla legge 5 giugno 1990, n. 135, per cui l'operatore sanitario e ogni altro soggetto che viene a conoscenza di un caso di Aids, ovvero di un caso di infezione da Hiv, anche non accompagnato da stato morboso, è tenuto a prestare la necessaria assistenza e as adottare ogni misura o accorgimento occorrente per la tutela dei diritti e delle libertà fondamentali dell'interessato, nonché della dignitiva dignità.

Capo II
Disposizioni transitorie

Art. 180 Misure di sicurezza

Questo articolo[111] conferma che le misure minime di cui al DPR 318/99 debbono comunque rimanere in vigore. Le misure minime, non previste dal Dpr 318/99, invece, entreranno in vigore a partire dal 31 dicembre 2005. Il titolare ed il responsabile del trattamento hanno quindi tempo fino a tale data per l'attuazione delle misure minime, ed, in casi assolutamente straordinari, che devono essere documentati in modo inoppugnabile, possono estendere tale tempo fino alla fine dell'anno 2005.

Art. 181 Altre disposizioni transitorie

Questo articolo, così come il precedente, individua una serie di fattispecie la cui regolamentazione va fatta non a decorrere dalla data di entrata in vigore del Codice ma successivamente. Si pensi: alle notificazioni dei trattamenti dei dati personali effettuati prima del 31.12.2003 che vanno compiute entro il 30 aprile 2004.

Art. 182 Ufficio del Garante

E' previsto il potenziamento dell'organico di tale Ufficio.

[111] Tale articolo è stato modificato dal Decreto Legge n. 314 del 30.12.2004.

Art. 183 Norme abrogate

Tale articolo contiene una lunga teoria di norme che all'entratat in vigore del presente codice sono abrogate.

Art. 184 Attuazioni di direttive europee

Attraverso tale codice si è inteso dare attuazione sia alla Direttiva 96/45CE, già recepita dalla Legge n. 675/96, che alla Direttiva 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

Art. 185 Allegazione dei codici di deontologia e di buona condotta

Al presente codice sono stati allegati i seguenti codici di deontologia e di buona condotta, redatti dagli organismi di categoria e approvati dal Garante:

- Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica
- Codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici
- Codice di deontologia e di buona condotta per il trattamento di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del sistema statistico nazionale

Art. 186 Entrata in vigore

Disciplina la entrata in vigore delle presenti disposizioni .

Autore: Dott. Giovanni Modesti