DIRETTORE	SIGLA ISTITUTO
Adorno Prof. Domenico	ITOI
Alemà Dr. Stefano (f.f.)	IBC
Alfano Dr. Bruno	IBB
Ambrosio Dr. Ing. Luigi	IMCB
Anfossi Dr. Domenico (f.f.)	ISAC
Angelini Dr. Giancarlo	IMC
Avaldi Dr. Lorenzo	IMIP
Avveduto Dr.ssa Sveva	IRPPS
Baldini Prof. Antonio	IGB
Belardini Dr.ssa Paola	IM
Beltrami Prof. Pietro	OVI
Bertsch Prof. Nichiel	IAC
Biamonti Dr. Giuseppe	IGM
Bianchini Dr. Claudio	ICCOM
Bollini Dr. Roberto	IBBA
Bolognesi Dr. Alberto	ISMAC
Bottino Dr.ssa Rosa Maria	ITD
Bozzi Dr. Andrea	ILC
Brezzi Prof. Franco	IMATI
Brugnoli Dr. Enrico (f.f.)	IBAF
Bucci Prof. Ovidio Mario	IREA
Burgyan Dr. Jozsef	IVV

Cacciola Dr. Gaetano	ITAE
Carfagna Prof. Cosimo	ICTP
Castelfranchi Prof. Cristiano	ISTC
Ceccotti Prof. Ario	IVALSA
Cellai Dr. Luciano (f.f.)	IC
Ciampi Dr. Costantino	ITTIG
Codignola Bo Prof. Luca	ISEM
Coppola Prof. Raffaele	ISA
Cucca Prof. Francesco	INN
Cuomo Prof. Vincenzo	IMAA
D'Andria Dr. Riccardo (f.f.)	ISAFoM
D'Andria Prof. Francesco	IBAM
Daolio Dr. Sergio	IENI
D'Atena Prof. Antonio	ISSIRFA
De Natale Dr. Paolo	INOA
De Portu Dr. Goffredo (f.f.)	ISTEC
Distante Dr. Arcangelo	ISSIA
Evangelisti Prof. Florestano	IFN
Fabri Dr. Marco (f.f.)	IRSIG
Fiorani Dr. Dino	ISM
Frediani Prof. Piero	ICVBC
Fusco Prof. Alfredo	IEOS

Gambacorta Dr. Agata	ICB
Gambale Dr. Franco	IBF
Gambardella Prof. Antonio	ISN
Garraffo Dr. Salvatore	ITABC
Germano' Prof. Alberto	IDAIC
Gianelli Dr. Giovanni	IGG
Giorno Dr.ssa Lidietta	ITM
Grandori Dr. Ferdinando	ISIB
Iannotta Dr. Salvatore	IMEM
Iannuzzi Dr. Leopoldo (f.f.)	ISPAAM
Laforenza Dr. Domenico	IIT
Lamarra Dr. Antonio (f.f.)	ILIESI
Lami Prof. Alessandro (f.f.)	IPCF
Lontano Dr. Maurizio Giuseppe	IFP
Malanima Prof. Paolo	ISSM
Maracchi Prof. Gianpiero	IBIMET
Marchisio Prof. Sergio	ISGI
Marconi Dr. Claudio (f.f.)	IBFM
Marra Dr.ssa Ersilia (f.f.)	IBBE
Mazzola Dr. Salvatore	IAMC
Mercanti Dr. Delio (f.f.)	INMM
Molinari Prof.ssa Elisa	INFM

Montani Dr. Claudio	ISTI
Morvillo Dr. Alfonso	IRAT
Mosello Dr. Rosario	ISE
Nucci Dr. Roberto Enrico (f.f.)	IBP
Padeletti Dr.ssa Giuseppina	ISMN
Pettine Dr. Maurizio	IRSA
Picano Dr. Eugenio	IFC
Pietronero Prof. Luciano	ISC
Pignone Dr. Domenico	IGV
Piovan Dr. Roberto	IGI
Pirastu Dr. Mario	IGP
Pirrone Prof. Nicola	IIA
Pozzan Prof. Tullio	IN
Psaro Dr. Rinaldo	ISTM
Rafanelli Ing. Claudio (f.f.)	IA
Rinaldi Dr. Giovanni	IASI
Riva Dr. Sergio	ICRM
Rolfo Dr. Secondo	CERIS
Rossetto Dr. Gilberto	ICIS
Rossi Dr. Pietro Mario (f.f.)	IDPA
Ruberti Dr.ssa Ida (f.f.)	IBPM
Salatino Prof. Piero	IRC

Salimbeni Dr. Renzo	IFAC
Sanna Dr.ssa Manuela (f.f.)	ISPF
Santoro Dr.ssa Paola	ISCIMA
Seconi Dr. Giancarlo	ISOF
Sorriso Valvo Dr. Giovanni Marino	IRPI
Spinella Dr. Rosario Corrado	IMM
Talia Prof. Domenico	ICAR
Tascone Dr. Riccardo	IEIIT
Termini Prof. Settimio	ICIB
Tolio Prof. Tullio Antonio Maria	ITIA
Trincardi Dr. Fabio	ISMAR
Turchetti Prof.Tullio (f.f.)	IPP
Vagnetti Dr.ssa Lucia (f.f.)	ICEVO
Viegi Dr. Giovanni	IBIM
Vinci Dr. Roberto	ITC
Visconti Dr. Angelo	ISPA
Zarotti Ing. Gian Luca	IMAMOTER
Zecca Dr. Luigi (f.f.)	ITB
Zuppi Prof. Giovanni Maria	IGAG

Consiglio Nazionale delle Ricerche
Direzione Generale

Circolare n. 4/2005

Pos. 6.9 Prot. n. 0032307
ns. rif.: S/DG/629

Roma, 16 giugno 2005

A Presidente
Responsabili degli Uffici di diretta collaborazione
Responsabili delle Direzioni Centrali
Dirigenti degli Uffici delle Direzioni Centrali
Direttori degli Istituti

LORO - SEDI

Oggetto: *Applicazione D.L.vo 30.6.2003, n. 196 – Codice in materia di protezione dei dati personali – adempimenti relativi.*

Ai sensi di quanto previsto dal D.lvo 30 giugno 2003 n. 196, "Codice in materia di protezione dei dati personali", ciascun titolare di trattamento di dati personali deve provvedere ad approntare, entro la scadenza perentoria del 30 giugno 2005, le misure minime di sicurezza previste dagli artt. da 31 a 36 e dal Disciplinare Tecnico allegato al Codice medesimo. Trattasi degli accorgimenti minimi strutturati al fine di scongiurare rischi di distruzione, perdita, manipolazione, utilizzo improprio o illecito dei dati trattati, indipendentemente dalla natura degli stessi, siano dunque comuni, sensibili o giudiziari. La mancata adozione delle misure minime di sicurezza costituisce, ai sensi di quanto previsto dall'art. 169 del Codice, illecito penale punibile con l'arresto fino a due anni o con l'ammenda da diecimila a cinquantamila euro.

Nell'ambito delle prescrizioni normative, innovativo e particolarmente rilevante risulta l'obbligo della redazione - qualora il titolare effettui il trattamento dei dati mediante strumenti automatizzati - di un Documento programmatico sulla Sicurezza, che contenga, fra l'altro:- l'elenco dei trattamenti dei dati personali;- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;- l'analisi dei rischi che incombono sui dati;- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia ed accessibilità;- la previsione di interventi formativi per gli incaricati del trattamento. Per consentire la redazione di suddetto documento, nonché al fine di approntare le più generali misure minime di sicurezza di cui sopra, si rappresenta, pertanto, la necessità, per questo Consiglio, di effettuare un generale censimento circa i trattamenti di dati personali effettuati in ciascuna struttura. A tale scopo si invia in allegato alle SS.LL. un apposito questionario, strutturato al fine di ottenere le informazioni di massima circa le specifiche attività di trattamento, le tipologie di dati trattati, i soggetti cui si riferiscono i dati, gli incaricati del trattamento nonché l'esistenza di misure di sicurezza già approntate. Il questionario di cui trattasi, disponibile in modello formato word, dovrà essere compilato a cura del responsabile della struttura e restituito, via posta elettronica all'indirizzo trattamentodati@cnr.it, e in forma cartacea alla Direzione Centrale Supporto alla Programmazione e alle Infrastrutture, p.le Aldo Moro, 7 – 00185 ROMA **entro e non oltre il 29 giugno 2005**.

Per ogni ulteriore informazione è possibile rivolgersi all'Avv. Luciano Marini Dirigente dell'Ufficio IV della Direzione Generale - tel 06.49932034, responsabile ai sensi del provvedimento del Presidente del CNR n. 33 del 26 maggio 2005, dell'applicazione in ambito CNR del D.Lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali".

Ringraziando per la collaborazione si inviano i più cordiali saluti.

IL DIRETTORE GENERALE

094

CONSIGLIO NAZIONALE DELLE RICERCHE

SCHEDA DI RILEVAZIONE DEI TRATTAMENTI DI DATI PERSONALI

STRUTTURA (*) _____

RESPONSABILE _____

(*) Amministrazione centrale; Istituti; Altro

Attività della struttura (1)	Natura dei dati trattati (2)	Soggetti cui si riferiscono i dati (3)	Descrizione del trattamento (4)	Modalità di trattamento (5)	Banche dati (eventuali) (6)	Incaricati del trattamento (7)

(1) Indicare le attività espletate dalla struttura (corrispondenti, normalmente alle competenze); es. gestione carriere personale, elezioni organi, ecc..

(2) Indicare se comuni, sensibili, o giudiziari.
Si rammenta in proposito che, ai sensi di quanto previsto dall'art. 4 del d.lgs. 196/2003 si intendono per **dati sensibili**, i dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale; per **dati giudiziari**, i dati personali idonei a rivelare la qualità di imputato o di indagato, il casellario giudiziale, l'anagrafe delle sanzioni amministrative dipendenti da reato e i relativi carichi pendenti.

(3) Indicare in dettaglio; es. personale dipendente o a contratto, fornitori, ecc.

(4) Indicare il tipo di operazioni effettuate sui dati; es. raccolta, registrazione, modifica, ecc.
Si rammenta in proposito che si intende per trattamento, ai sensi di quanto previsto dall'art. 4 lett. a del d.lgs. 196/2003, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

(5) Indicare se cartaceo, informatico o misto.

(6) Indicare la denominazione, qualora i dati siano organizzati in una banca dati.

(7) Indicare le persone fisiche autorizzate al trattamento dei dati (anche eventuale personale esterno). E possibile, qualora sia incaricato al trattamento l'intero personale della struttura, indicare riassuntivamente " tutto il personale della struttura".

LUOGO DI CUSTODIA DEI DATI

- Trattamento cartaceo (indicare l'ubicazione fisica degli archivi)

- Trattamento informatizzato (indicare l'ubicazione fisica dei supporti di memorizzazione, ossia l'elaboratore sui cui dischi sono memorizzati i dati - barrare la/e casella/e di interesse):
-
  - ❑ *presso la struttura (pc/server)*
  - ❑ *altro (specificare).*

MISURE DI SICUREZZA ESISTENTI

- Fisiche (barrare la/e casella/e di interesse) :
  - ❑ *Arredi chiudibili a chiave*
  - ❑ *Identificazione degli accessi agli archivi*

- Elettroniche (barrare la/e casella/e di interesse)
  - ❑ *Autenticazione informatica (login per l'accesso alla rete/ computer)*
  - ❑ *Sistema di autorizzazione (login per l'accesso alla specifiche applicazioni informatiche)*
  - ❑ *Dispositivi di salvataggio dati(backup)*
  - ❑ *Antivirus/firewall*
  - ❑ *Criptazione dati sensibili*

Roma/Sede della struttura,

IL RESPONSABILE DELLA STRUTTURA

Consiglio Nazionale delle Ricerche
Direzione Generale

Circolare n. 13/2005

RIF. N. 0066110 DEL 27/12/2005

Ai Sig.ri
Presidente
Vice Presidente
Responsabili degli Uffici di diretta collaborazione
Responsabili delle Direzioni Centrali
Dirigenti degli Uffici delle Direzioni Centrali

Direttori degli Istituti
Presidenti delle Aree di Ricerca

LORO SEDI

Oggetto: *D.lvo 196/2003 Adempimenti organizzativi e nomine dei Responsabili del trattamento dei dati personali.*

In considerazione dell'entrata in vigore, il 1° gennaio 2004, del decreto legislativo 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali), e degli obblighi e adempimenti ad esso inerenti (in particolare l'obbligo di redazione del Documento Programmatico sulla Sicurezza), è emersa la necessità di dar corso ad una razionalizzazione dell'assetto organizzativo del CNR, in materia di tutela delle persone e di altri soggetti nel trattamento dei dati personali, cui in prima istanza si è provveduto con l'adozione della deliberazione del Consiglio di Amministrazione n.115/2005 del 27 luglio 2005, che viene allegata in copia. Dovendosi ora procedere all'attuazione , si precisano con la presente circolare, le istruzioni dirette ai responsabili dei trattamenti.

In proposito si rammenta che, ai sensi di legge, sono soggetti preposti al trattamento dei dati personali:

il Titolare identificato nella persona fisica, giuridica o pubblica amministrazione cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Nell'ipotesi di trattamento da parte di pubblica amministrazione la titolarità è in capo all'ente nel suo complesso.

Il Consiglio Nazionale delle Ricerche è, pertanto," titolare " dei dati personali da esso trattati con l'ausilio dei mezzi cartacei e/o informatici.

I Responsabili ossia i soggetti individuati dal titolare che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Ai sensi di quanto previsto dal vigente Regolamento di Organizzazione e Funzionamento del Consiglio Nazionale delle Ricerche si individuano come responsabili del trattamento dei dati personali i responsabili pro-tempore delle strutture scientifiche e di servizio in cui si articola il CNR.

La nomina a responsabile è effettuata, in sede di prima applicazione della normativa di riferimento, con apposito provvedimento.

094

A regime, la nomina a responsabile del trattamento dei dati personali sarà contestuale al decreto (o altro provvedimento) di nomina alla direzione della struttura.

Gli incaricati ossia le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dai responsabili.

La designazione degli incaricati va effettuata per iscritto e deve individuare puntualmente l'ambito del trattamento consentito. Si considera tale tuttavia anche la documentata preposizione della persona fisica all'Unità Organizzativa per la quale è stato individuato per iscritto, l'ambito del trattamento consentito agli addetti dell'Unità Organizzativa

Nell'ambito del CNR, per quanto riguarda il personale di ruolo (personale tecnico amministrativo e ricercatore)e personale operante ad altro titolo (personale a contratto, dottorandi, titolari di assegni di ricerca) nell'Unità Organizzativa sulla base di provvedimento o atto formale, l'obbligo di designazione scritta è stato assolto mediante l'indicazione dei medesimi all'interno delle schede di rilevazione dei trattamenti inviate in risposta alla circolare n. 4/05 pos 6.9 prot. 0032307 del 16 giugno 2005.
Qualora il responsabile, nello svolgimento delle sue funzioni istituzionali, ritenga necessario autorizzare soggetti diversi dai precedenti al trattamento dei dati personali inerenti la sua struttura, dovrà provvedere a designare individualmente per iscritto i medesimi.

In relazione a quanto detto, sarà trasmesso l'atto individuale di nomina a responsabile del trattamento dei dati personali.

L'ambito di responsabilità si estende al trattamento dei dati effettuati, sia con l'ausilio di strumenti elettronici che in maniera cartacea, nell'ambito dell'Unità Organizzativa di riferimento e si riferisce alla tipologie di dati e di trattamenti indicati nell'apposita scheda di rilevazione del trattamento fornita in risposta alla circolare n. 4/05 del 16 giugno 2005.

Sulla base delle informazioni fornite tramite le schede di cui trattasi, sarà creata una apposita banca dati denominata "anagrafe elettronica dei trattamenti", che costituirà, a regime, il preciso riferimento circa i trattamenti di dati personali effettuati in ciascuna struttura, il responsabile degli stessi, gli incaricati di ciascun trattamento nonché le misure di sicurezza in essere.

Sarà cura di ciascun responsabile del trattamento provvedere, a regime, ad inviare i dati per l'aggiornamento al competente Ufficio dell'Amministrazione Centrale, Ufficio che sarà successivamente indicato, ove cambi qualcuna delle indicazioni in essa contenute, ovvero procedere almeno annualmente alla ricognizione circa la validità dei dati in essa contenuti.

I compiti di spettanza di ciascun responsabile sono analiticamente specificati nell'atto di nomina.

Si rammenta che, allo scopo di rappresentare in un quadro unitario il complesso delle misure organizzative, logistiche, tecniche, ed informatiche da adottarsi all'interno del CNR, è stato predisposto un apposito "Manuale per la sicurezza ed il corretto trattamento dei dati personali nel Consiglio Nazionale delle Ricerche", disponibile in intranet all'indirizzo http://www.cnr.it , del quale si prega di prendere accurata conoscenza e diffondere tra i propri collaboratori.

Per ogni ulteriore informazione è possibile rivolgersi a:

1. Avv. Luciano Marini - Dirigente Ufficio IV- Direzione Generale – tel. 06 49932034 – per chiarimenti di carattere organizzativo e/o giuridico-normativo;
2. Ing. Mario Tozzoli –Dirigente Ufficio Reti e Telecomunicazioni della DCSPI tel.06 49933625 per chiarimenti ed informazioni di carattere tecnico informatico.

094

Ringraziando per la collaborazione si inviano i più cordiali saluti.

IL DIRETTORE GENERALE

094

REPVBBLICA ITALIANA

Consiglio Nazionale delle Ricerche

Misure urgenti in materia di trattamento dei dati personali- Ratifica

Il Consiglio di Amministrazione nella riunione in data 27 luglio 2005, ha adottato all'unanimità la seguente deliberazione n. 115/2005 - Verb. 22

IL CONSIGLIO DI AMMINISTRAZIONE

- visto il Decreto Legislativo n. 127 del 4 giugno 2003, recante disposizioni sul "Riordino del Consiglio Nazionale delle Ricerche", ed in particolare l'art. 6, comma 1, lettera e);
- visto il Regolamento di organizzazione e funzionamento del Consiglio Nazionale delle Ricerche, emanato con decreto del Presidente del 4 maggio 2005, prot. n. 25033 e pubblicato nel Supplemento ordinario n. 101 alla Gazzetta Ufficiale della Repubblica Italiana n. 124 del 30 maggio 2005, ed in particolare l'art. 3 comma 2 lettera f);
- visto il decreto del Presidente prot. n. 0034935 del 1° luglio 2005, con il quale è stato approvato il disciplinare sul trattamento dei dati personali comuni e sensibili;
- viste in particolare le motivazioni del predetto decreto da intendersi qui integralmente trascritte;
- ritenuti validi i motivi d'urgenza;

DELIBERA

- di ratificare l'allegato decreto del Presidente prot. n. 0034935 in data 1° luglio 2005.

IL PRESIDENTE
f.to Fabio Pistella

IL SEGRETARIO
f.to Giuliano Salberini

CONSIGLIO NAZIONALE DELLE RICERCHE

Copia conforme all'originale
UFFICIO DEL PRESIDENTE
IL RESPONSABILE
(Dott. Giuliano SALBERINI)
IL PRESENTE DOCUMENTO
SI COMPONE DI N°...../.... PAGINE

Roma, 8 SET. 2005

094

REPVBBLICA ITALIANA

Consiglio Nazionale delle Ricerche

Pos. 6.9 Prot. 0034935 Data - 1 LUG. 2005

Misure urgenti in materia di trattamento dei dati personali

Provvedimento n. 054

IL PRESIDENTE

- visto il D.lgs. 4 giugno 2003 n. 127, recante "Riordino del Consiglio Nazionale delle Ricerche";

- visto il D.lgs 30 giugno 2003, n.196, Codice in materia di protezione dei dati personali;

- vista la direttiva del Ministro per la funzione pubblica del 11 febbraio 2005 "Misure finalizzate all'attuazione delle disposizioni contenute nel D.Lgs. 30 giugno 2003, n.196, recante il Codice in materia di protezione dei dati personali";

- visti i Regolamenti di Organizzazione e funzionamento, Amministrazione Contabilità e Finanza e del Personale del Consiglio Nazionale delle Ricerche (CNR), pubblicati nel Supplemento ordinario n. 101 alla Gazzetta Ufficiale della Repubblica Italiana n.124 del 30 maggio 2005;

- visto il decreto del Presidente n.33 del 26 maggio 2005 che conferisce, tra l'altro anche in vista dell'entrata in vigore dei regolamenti un incarico all'avv. Luciano Marini, consigliere giuridico del direttore generale, di formulare proposte dirette ad assicurare il pieno adempimento delle disposizioni sul trattamento dei dati personali;

- preso atto che a seguito dell'entrata in vigore dei regolamenti del CNR con lettera circolare del direttore generale prot. 232307 del 16 giugno 2005, predisposta dall'avv. Luciano Marini in base al citato incarico, si è avviata una ricognizione nelle strutture dell'Ente centrali e periferiche dei trattamenti effettuati anche al fine di assicurare l'adempimento delle prescrizioni di legge in materia di adozione di misure minime di sicurezza nel più generale contesto del trattamento dei dati personali;

- vista la nota del dirigente incaricato, avv. Luciano Marini, prot. 945/05 del 23 giugno 2005 nella quale si dà una informativa sull'attività svolta;

- ravvisata l'esigenza di assicurare in coerenza con i termini fissati dal D.lgs 30 giugno 2003, n.196, come modificati dalla legge 1 marzo 2005, n.26 di conversione del decreto legge 30 dicembre 2004, n.314, e con le specificità del nuovo assetto organizzativo, che siano compiutamente definiti con atto regolamentare i criteri generali e le procedure per l'applicazione delle disposizioni sul trattamento dei dati personali, con particolare riguardo alle misure minime di sicurezza che entreranno in vigore il 31 dicembre 2005;

- rilevata la complessità, anche con riferimento alle puntualizzazioni espresse nella citata direttiva del Dipartimento della funzione Pubblica circa la necessità per le amministrazioni di ripensare la propria organizzazione al fine di consentire una piena ed effettiva garanzia dei diritti riconosciti dalla legge e alle dinamiche di riassetto dell'Ente, che richiede qualche mese di approfondimento per completare la predisposizione di un atto regolamentare definitivo;

- ravvisata l'urgenza di codificare fin d'ora alcune regole con un disciplinare da approvare a stralcio per rendere uniforme all'interno dell'Ente l'applicazione alcune misure già in uso e definire funzioni e responsabilità in materia immediatamente operative;

- ritenuto opportuno affidare ad un gruppo ristretto in cui siano presenti le necessarie professionalità i compiti di redigere un atto regolamentare che integri, se necessario, il disciplinare di cui al presente decreto per conseguire il completo adeguamento dell'Ente alle nuove prescrizioni entro il termine del 31 dicembre 2005, e assicuri l'applicazione delle disposizioni contenute nella Parte I, Titolo III, Capo II, "Regole ulteriori per i soggetti pubblici", ed in particolare le prescrizioni di cui all'articolo 20 del D.lgs 30 giugno 2003, n.196, anche in relazione alle dinamiche della riorganizzazione dell'Ente;

- ritenuto altresì di dover affidare al suddetto gruppo il compito di fornire, su richiesta del direttore generale, supporto nello sviluppo delle applicazioni informatiche e nella definizione dei processi organizzativi, per l'applicazione delle disposizioni in materia di trattamento dei dati personali;

- ritenuto altresì opportuno in questa fase attribuire al Direttore generale le competenze per conto del titolare Consiglio Nazionale delle Ricerche, come amministrazione nel suo complesso stabilendo al suo interno le responsabilità di massima;

- ravvisata l'esigenza di attribuire al direttore generale il compito di intrattenere, avvalendosi del supporto del citato gruppo ristretto, rapporti con l'Autorità Garante e con altri Enti di ricerca per le questioni attinenti all'applicazione delle normative sul trattamento dei dati personali;

DECRETA

Art. 1

(Approvazione del disciplinare)

1. E' approvato il disciplinare sul trattamento dei dati personali comuni e sensibili di cui all'allegato A che costituisce parte integrante del presente decreto.

Art. 2

(Istituzione di un gruppo ristretto)

1. Il direttore generale istituisce presso la direzione generale un gruppo ristretto assicurando la presenza delle professionalità necessarie per svolgere le seguenti funzioni:

a) predisporre uno schema di atto regolamentare per l'individuazione di procedure e criteri generali per l'applicazione delle norme sul trattamento dei dati personali e per l'applicazione dell'articolo 20 del D.lgs 30 giugno 2003, n.196;

b) fornire supporto, su richiesta del direttore generale, nelle attività di sviluppo delle applicazioni informatiche e di definizione dei processi organizzativi, per l'applicazione delle disposizioni in materia di trattamento dei dati personali.

2. Il direttore generale intrattiene i rapporti con l'Autorità Garante per il Trattamento dei Dati Personali e con altri Enti di ricerca per le questioni attinenti all'applicazione delle normative sul trattamento dei dati personali avvalendosi del supporto del gruppo ristretto.

3. Per quanto riguarda le attività di cui al comma 1 lettera a) il gruppo di lavoro presenterà una proposta al direttore generale entro il 30 ottobre 2005.

REPVBBLICA ITALIANA

Consiglio Nazionale delle Ricerche

Art. 3

(Ratifica)

1. Il presente decreto è sottoposto a ratifica del Consiglio di amministrazione a norma dell'articolo 3 comma 2 lettera f) del Regolamento di organizzazione e funzionamento.

IL PRESIDENTE

ALLEGATO A

DISCIPLINARE SUL TRATTAMENTO DEI DATI PERSONALI COMUNI E SENSIBILI DEL CONSIGLIO NAZIONALE DELLE RICERCHE

CAPO I DISPOSIZIONI GENERALI

ART. 1 OGGETTO

1. Le norme di cui al presente disciplinare regolano il trattamento dei dati personali effettuato dal Consiglio Nazionale delle Ricerche (CNR) in attuazione delle disposizioni vigenti in materia.

ART. 2 FINALITA'

1. Il CNR garantisce che il trattamento dei dati comuni e sensibili, sia effettuato esclusivamente nello svolgimento delle proprie attività istituzionali nel rispetto delle norme sul trattamento dei dati personali nell'ambito delle amministrazioni pubbliche e, in particolare, degli enti di ricerca.

2. Ai fini dell'applicazione del presente disciplinare per attività istituzionali si intendono:
   a) le attività previste dal leggi e regolamenti;
   b) le attività svolte in base a intese, convenzioni e accordi volti all'espletamento di funzioni istituzionali;
   c) le attività di rilevante interesse pubblico come definite dalla normativa vigente e i relativi trattamenti.

ART. 3 DEFINIZIONI

1. Per le definizioni di banca dati, trattamento, dato personale, titolare, responsabile, incaricato, interessato, comunicazione, diffusione, dato anonimo, blocco, si fa riferimento a quanto previsto dall'art.4, comma 1 del D.lgs 30 giugno 2003, n.196 e dal D.P.R. 318/99. Per dati si intendono dati comuni e sensibili e specificatamente quelli inerenti alla salute.

ART. 4 CAMPO DI APPLICAZIONE

1. Le disposizioni del presente disciplinare si applicano al trattamento automatizzato e non, dei dati personali, attuato nell'ambito del CNR. Esso può distinguersi in:
   a) trattamento dei dati personali "comuni"' realizzato per lo svolgimento delle attività istituzionali nei limiti stabiliti dalla legge o dai regolamenti;
   b) trattamento dei dati "sensibili" autorizzato da espresse disposizioni di legge.

CAPO SECONDO

DISPOSIZIONI ORGANIZZATIVE

ART. 5 TITOLARE E RESPONSABILI

1. Il titolare delle banche dati é il CNR nella persona del suo Direttore Generale.

2. I responsabili preposti al trattamento dei dati sono nominati dal titolare e vengono scelti tra il personale che per esperienza, capacità ed affidabilità, possa fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. I trattamenti, cui la responsabilità si riferisce, sono quelli afferenti l'area di attività del dipendente e/o, comunque, connessi alle funzioni assolte e agli incarichi ricoperti.

3. Ai responsabili competono:
a) Il rispetto delle istruzioni di carattere generale fornite dal titolare.
b) La predisposizione di ogni atto ed operazione necessarie al rispetto dei obblighi:
   1) notificazione e comunicazione al garante (ove necessaria);
   2) informativa all'interessato relativa al trattamento, comunicazione e diffusione dei dati;
   3) acquisizione dell'eventuale consenso;
   4) rispetto delle modalità generali di raccolta dei dati e dei requisiti dello stesso, nonché delle specifiche disposizioni relative a trattamenti particolari;
   5) richiesta di autorizzazione al garante per i trattamenti di dati sensibili non disciplinati dalla legge;
   6) adempimenti connessi alla cessazione dei trattamenti;
   7) adozione di adeguate misure di sicurezza anche con l'apporto del responsabile del Sistema Informativo;
   8) formale individuazione dei destinatari di eventuali sub deleghe;
   9) vigilanza sull'osservanza della legge da parte dei propri incaricati.

ART. 6 NOMINA DEGLI INCARICATI

1. Il responsabile del trattamento dei dati può procedere alla formale individuazione, all'interno di ciascuna area operativa degli incaricati, ossia delle persone autorizzate nella varie Unità operativa a compiere le operazioni di trattamento dei dati, da svolgersi secondo le modalità di cui agli art.11 e 12 del D.lgs 30 giugno 2003, n.196.

2. I compiti affidati agli incaricati devono essere specificati dal responsabile che ne controlla l'osservanza.

3. Gli incaricati del trattamento devono effettuare le operazioni loro affidate attenendosi alle istruzioni ricevute. Essi devono fornire idonee garanzie in merito alle misure di sicurezza tecnica ed organizzativa dei trattamenti da effettuare.

CAPO TERZO

DISPOSIZIONI PROCEDURALI

ART. 7 TRATTAMENTO DEI DATI

1. Il CNR tratta dati comuni per lo svolgimento delle proprie attività istituzionali nel rispetto dei limiti stabiliti dalla legge e dai regolamenti. I dati devono essere:
   a. trattati in modo lecito e secondo correttezza;
   b. raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati solo al fine del raggiungimento di tale scopo istituzionale;
   c. esatti e, se necessario, aggiornati;
   d. pertinenti, completi e non ridondanti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati
   e. conservati in una forma che consenta la identificazione immediata dell'interessato per un periodo di tempo non superiore a quella necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati.

2. I dati contenuti in elenchi, registri e banche-dati, tenuti con l'ausilio di mezzi elettronici o, comunque, automatizzati, sono trattati con tecniche di criptazione o mediante l'utilizzazione di codici identificativi o di altri sistemi che, considerato il numero e la natura dei dati trattati permettano di identificare gli interessati solo in caso di necessità e garantiscano la protezione da illecite intromissioni secondo quanto previsto dall'art. 4 del D.P.R. 318/99.

3. I dati idonei a rilevare lo stato di salute e la vita sessuale sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo. Al trattamento di tali dati si procede con le modalità di cui al comma 6 dell'art. 22 del del D.lgs 30 giugno 2003, n.196 indipendentemente dal supporto e dal sistema di conservazione e gestione utilizzato.

4. Il trattamento dei dati deve essere effettuato adottando misure tecniche ed organizzative atte a garantirne la riservatezza e la protezione da ogni forma illecita di trattamento.

5. Tali misure devono assicurare un livello di sicurezza appropriato rispetto ai rischi connessi al trattamento ed alla natura dei dati da proteggere e devono essere aggiornate in rapporto e relazione all'evoluzione tecnologica e legislativa in materia.

ART. 8 SOGGETTI TERZI

1. Il trattamento dei dati acquisiti nell'ambito delle attività istituzionali del CNR può essere effettuato, nei limiti strettamente pertinenti agli obblighi, compiti e finalità, da:

a) ditte, imprese, società, consorzi o associazioni che per conto del CNR forniscono specifici servizi o che svolgono attività connesse, strumentali o di supporto a quelle del CNR medesima ovvero attività necessarie alla esecuzione di prestazioni e di servizi imposti da disposizioni di legge o attivati al fine di soddisfare bisogni e richieste di cittadini;
b) soggetti ai quali la comunicazione dei dati risulta necessaria per lo svolgimento delle attività affidate dal CNR;
c) soggetti cui la facoltà di accedere ai dati sia riconosciuta da disposizioni di legge o di regolamento. In quest'ultimo caso si applica l'art. 22 comma 11 del D.lgs 30 giugno 2003, n.196.

2. Tra i servizi istituzionali del CNR rientrano anche le funzioni svolte su delega convenzioni o concessioni da soggetti pubblici o privati, nonché dagli Istituti di credito che operano come tesorieri.

3. Nei casi sopra indicati il soggetto che effettua il trattamento per conto del CNR è tenuto ad osservare sia gli obblighi e le misure di sicurezza previste dal D.lgs 30 giugno 2003, n.196, sia le direttive impartite dal titolare o dal responsabile, nonché ogni altra disposizione derivante da norme sul trattamento dei dati sensibili e di salute.

4. I trattamenti dei dati effettuati, da terzi per conto del CNR sono disciplinati da atti o provvedimenti che devono indicare la qualifica del soggetto terzo, titolare, responsabile o incaricato, a seconda dei casi, cui deve seguire, ove prevista, la formale nomina ai sensi di legge del soggetto stesso. All'atto della nomina devono essere indicate a carico del Soggetto terzo opportune prescrizioni, aggiornate periodicamente.

5. Ai fini della conservazione delle prove, gli elementi del contratto o dell'atto giuridico relativo alla protezione dei dati ed i requisiti concernenti le misure di cui sopra, devono essere formulate per iscritto.

ART. 9 MISURE DI SICUREZZA E AMMINISTRATORE DI SISTEMA

1. L'Amministratore di Sistema provvede, ai sensi degli artt. 4 e 5 del DPR 318/99, all'adozione di idonee misure di sicurezza al fine di:

a) prevenire i rischi di distruzione, alterazione o perdita dei dati o danneggiamento all'hardware e ai locali nei quali esso è custodito. Ai fini della definizione di hardware, software e dell'adozione del relativo regime generale di tutela vale quanto prescritto dalla normativa specifica in materia ed, in particolare, dalla L. 547/93.
b) prevenire l'accesso non autorizzato, anche mediante l'adozione di password e/o codici di identificazione disattivabili all'occorrenza;
c) definire le modalità di trattamento dei dati e le misure atte a prevenire l'accesso non autorizzato alle banche dati, alle reti e, in generale, agli strumenti informatici dell'Ente.

3. L'Amministratore di Sistema cura inoltre la revisione semestrale dei programmi e delle procedure di sicurezza di cui al comma 1.

4. L'Amministratore di Sistema predispone annualmente – con la collaborazione del Responsabile dell'Archivio e degli incaricati delle varie unità operative - il Documento programmatico della sicurezza dei dati ai sensi dell'art.6 del DPR 318/99. In esso va ricompresa la valutazione dei rischi e la distribuzione dei compiti e delle responsabilità relativamente non solo del materiale informatico o trattato per via telematica ma anche dei documenti e degli archivi cartacei anche in considerazione di quanto prescritto dal D.lgs. 7 marzo 2005, n.82, Codice dell'amministrazione digitale.

ART. 10 INFORMAZIONE

1. L'Amministratore di Sistema deve dare la più ampia diffusione ed attuazione agli obblighi informativi di cui all'art.13 del D.lgs 30 giugno 2003, mediante metodi e sistemi che le situazioni contingenti riveleranno idonei al migliore raggiungimento dello scopo istituzionale prefissato dalla norma.

ART. 11 DIRITTI DELL'INTERESSATO

1. I soggetti interessati al trattamento dei dati personali che intendono esercitare i diritti di cui all'art.7 del del D.lgs 30 giugno 2003, n.196 indirizzano le relative istanze all'Amministratore di Sistema anche tramite l'Ufficio Relazioni con il Pubblico.

ART. 12 NORME FINALI

1. Le procedure di dettaglio adottate dalle singole unità operative per dare piena applicazione al D.lgs 30 giugno 2003, n.196 ed al presente disciplinare sono comunicate al direttore generale che con proprio atto provvede ove lo ritenga a formalizzarle quali istruzioni di carattere generale fornite dal titolare.

Garante per la protezione
dei dati personali

PROVVEDIMENTO generale del 29 novembre 2000

Videosorveglianza. Il decalogo delle regole per non violare la privacy

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice-presidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti e del dott. Giovanni Buttarelli, segretario generale;

Viste le numerose note pervenute in merito alla conformità alle disposizioni della legge 31 dicembre 1996, n. 675 di alcune iniziative volte ad installare sistemi ed apparecchiature di controllo video;

Visti gli atti d'ufficio e le osservazioni formulate ai sensi dell'art. 15 del regolamento n. 1/2000, adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicano sulla G.U. n. 162 del 13 luglio 2000;

Relatore il prof. Ugo De Siervo;

PREMESSO:

Questa Autorità ha ricevuto numerose richieste in merito alle cautele necessarie per conformare alla legge 31 dicembre 1996, n. 675, gli impianti di videosorveglianza stabili o comunque non occasionali, cioè l'installazione di sistemi, reti ed apparecchiature che permettono la ripresa e l'eventuale registrazione di immagini, in particolare a fini di sicurezza, di tutela del patrimonio, di controllo di determinate aree e di monitoraggio del traffico o degli accessi di veicoli nei centri storici.

Il Garante si è espresso sul tema in diverse occasioni formulando vari pareri e segnalazioni menzionati nella Relazione al Parlamento e al Governo per il 1999, consultabili sul sito *www.garanteprivacy.it* e sul bollettino dell'Autorità "*Cittadini e società dell'informazione*".

La tematica è stata esaminata da questa Autorità per i profili di sua competenza, ovvero per quanto riguarda la liceità e la correttezza del trattamento di dati personali.

In presenza di una crescente utilizzazione di impianti di videosorveglianza da parte di molti soggetti pubblici e privati, il Garante, nell'attesa di una specifica legislazione, reputa necessario sintetizzare gli adempimenti, le garanzie e le tutele già necessari in base alle norme vigenti, per facilitarne la conoscenza da parte degli operatori interessati.

Le regole di base della disciplina sul trattamento dei dati personali, infatti, sono già applicabili alle immagini ed ai suoni, qualora le apparecchiature che li rilevano permettano di identificare, in modo diretto o indiretto, i soggetti interessati.

Chi intende svolgere attività di videosorveglianza deve quindi osservare almeno le seguenti cautele, rispettando comunque il principio di proporzionalità tra mezzi impiegati e fini perseguiti:

1. Tutti gli interessati devono determinare esattamente le finalità perseguite attraverso la videosorveglianza e verificarne la liceità in base alle norme vigenti. Se l'attività è svolta in presenza di un pericolo concreto o per la prevenzione di specifici reati, occorre rispettare le competenze che le leggi assegnano per tali fini solo a determinate amministrazioni pubbliche, prevedendo che alle informazioni raccolte possano accedere solo queste amministrazioni.

2. Il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi (art. 9, comma 1, lett. a) e b), legge 675/1996).

3. Nei casi in cui la legge impone la notificazione al Garante dei trattamenti di dati personali effettuati da determinati soggetti (art. 7 legge 675/1996), questi devono indicare fra le modalità di trattamento anche la raccolta di informazioni mediante apparecchiature di videosorveglianza. Non è prevista alcuna altra forma di specifica comunicazione o richiesta di autorizzazione al Garante.

4. Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza, fornendo anche le informazioni necessarie ai sensi dell'art. 10 della legge n. 675/1996. Ciò è tanto più necessario quando le apparecchiature non siano immediatamente visibili.

5. Occorre rispettare scrupolosamente il divieto di controllo a distanza dei lavoratori e le precise garanzie previste al riguardo (art. 4 legge 300/1970).

6. Occorre rispettare i princìpi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando - quando non indispensabili - immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.

7. Occorre determinare con precisione il periodo di eventuale conservazione delle immagini, prima della loro cancellazione, e prevedere la loro conservazione solo in relazione a illeciti che si siano verificati o a indagini delle autorità giudiziarie o di polizia.

8. Occorre designare per iscritto i soggetti - responsabili e incaricati del trattamento dei dati (artt. 8 e 19 della legge 675/1996) - che possono utilizzare gli impianti e prendere visione delle registrazioni, avendo cura che essi accedano ai soli dati personali strettamente necessari e vietando rigorosamente l'accesso di altri soggetti, salvo che si tratti di indagini giudiziarie o di polizia.

9. I dati raccolti per determinati fini (ad esempio, ragioni di sicurezza, tutela del patrimonio) non possono essere utilizzati per finalità diverse o ulteriori (ad esempio, pubblicità, analisi dei comportamenti di consumo), salvo le esigenze di polizia o di

giustizia, e non possono essere diffusi o comunicati a terzi.

10. I particolari impianti per la rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato devono essere conformi anche alle disposizioni contenute nel d.P.R. 250/1999. E' altresì necessario che la relativa documentazione sia conservata per il solo periodo necessario per contestare le infrazioni e definire il relativo contenzioso e che ad essa si possa inoltre accedere solo a fini di indagine giudiziaria o di polizia.

Per gli impianti di videosorveglianza finalizzati esclusivamente alla sicurezza individuale (ad esempio, il controllo dell'accesso alla propria abitazione) si ricorda che questi non rientrano nell'ambito dell'applicazione della legge 675/1996, ricorrendo le condizioni di cui all'art. 3. Occorre, però, che le riprese siano strettamente limitate allo spazio antistante tali accessi, senza forme di videosorveglianza su aree circostanti e senza limitazioni delle libertà altrui. Occorre inoltre che le informazioni raccolte non siano in alcun modo comunicate o diffuse. Altrimenti si rientra nell'ambito di applicazione generale della legge 675/1996 e devono, quindi, essere rispettate tutte le indicazioni di cui ai punti precedenti.

TUTTO CIO' PREMESSO IL GARANTE:

segnala ai titolari del trattamento interessati, ai sensi dell'art. 31, comma 1, lett. c), della legge n. 675/1996, la necessità di conformare il trattamento dei dati ai princìpi della legge n. 675/1996 richiamati nel presente provvedimento.

Roma, lì 29 novembre 2000

IL PRESIDENTE

IL RELATORE

IL SEGRETARIO GENERALE

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimenti a carattere generale - 29 aprile 2004 Bollettino del n. 49/aprile 2004, pag. 0

[doc. web n. 1003482]

[doc. web. n. 1116810]

[v. anche Comunicato stampa]

Videosorveglianza - Provvedimento generale

Sommario

094

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visti gli atti d'ufficio e le osservazioni formulate ai sensi dell'art. 15 del regolamento n. 1/2000;

Relatore il prof. Gaetano Rasi;

RILEVATO

1. PREMESSA

Il Garante ritiene opportuno aggiornare e integrare il provvedimento del 29 novembre 2000 *(c.d. "decalogo" pubblicato sul Bollettino del Garante n. 14/15, p. 28)*, anche per conformare i trattamenti di dati personali mediante videosorveglianza al Codice entrato in vigore il 1° gennaio 2004 e ad altre disposizioni vigenti *(art. 154, comma 1, lett. c), d.lg. 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali)* che hanno rafforzato le garanzie per i cittadini. Per altro verso va evidenziato che nel triennio di applicazione del predetto provvedimento sono stati sottoposti all'esame dell'Autorità numerosi casi, attraverso reclami, segnalazioni e richieste di parere, i quali evidenziano un utilizzo crescente, spesso non conforme alla legge, di apparecchiature audiovisive che rilevano in modo continuativo immagini, eventualmente associate a suoni, relative a persone identificabili, spesso anche con registrazione e conservazione dei dati.

Con riferimento alle menzionate garanzie, il presente provvedimento (paragrafi 2 e 3) richiama taluni principi e illustra le prescrizioni generali relative a tutti i sistemi di videosorveglianza; nei paragrafi 4, 5 e 6 vengono invece individuate prescrizioni riguardanti specifici trattamenti di dati. Ovviamente, per casi particolari l'Autorità si riserva di intervenire di volta in volta con atti *ad hoc*.

Le prescrizioni del presente provvedimento hanno come presupposto il rispetto dei diritti e delle libertà fondamentali dei cittadini e della dignità delle persone con particolare riferimento alla riservatezza, all'identità ed alla protezione dei dati personali *(art. 2, comma 1, del Codice)*.

Il Garante ha posto doverosa attenzione al nuovo diritto alla protezione dei dati personali *(art. 1 del Codice)* consapevole che un'idonea tutela dei diritti dei singoli, oggetto del bilanciamento effettuato con il presente provvedimento, non pregiudica l'adozione di misure efficaci per garantire la sicurezza dei cittadini e l'accertamento degli illeciti.

Si è avuto riguardo pertanto anche alla libertà di circolazione nei luoghi pubblici o aperti al pubblico. In tali ambiti, non si possono privare gli interessati del diritto di circolare senza subire ingerenze incompatibili con una libera società democratica *(art. 8 Conv. europea diritti uomo ratificata con l. n. 848/1955)*, derivanti da rilevazioni invadenti ed oppressive riguardanti presenze, tracce di passaggi e spostamenti, facilitate dalla crescente interazione dei sistemi via Internet ed Intranet.

Il Garante si è infine ispirato alle indicazioni espresse in varie sedi internazionali e comunitarie: in particolare alle linee-guida del Consiglio d'Europa del 20-23 maggio 2003 *(v. Relazioni annuali del Garante per il 2002 e per il 2003, in www.garanteprivacy.it)*, nonché agli indirizzi formulati dalle autorità europee di protezione dei dati riunite nel Gruppo istituito dalla direttiva n. 95/46/CE *(11 febbraio 2004, n. 4/2004, in Relaz. annuale 2003 e http://europa.eu.int/comm/internal-market/privacy/workingroup/wp2004/wpdocs04_en.htm)*.

2. PRINCIPI GENERALI

2.1 Principio di liceità

Il trattamento dei dati attraverso sistemi di videosorveglianza è possibile solo se è fondato su uno dei presupposti di liceità che il Codice prevede espressamente per gli organi pubblici da un lato (svolgimento di funzioni istituzionali: *artt. 18-22*) e, dall'altro, per soggetti privati ed enti pubblici economici (adempimento ad un obbligo di legge, provvedimento del Garante di c.d. "bilanciamento di interessi" o consenso libero ed espresso: artt. 23-27). Si tratta di presupposti operanti in settori diversi e che sono pertanto richiamati separatamente nei successivi paragrafi del presente provvedimento relativi, rispettivamente, all'ambito pubblico e a quello privato.

La videosorveglianza deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati, di quanto prescritto da altre disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi.

Vanno richiamate al riguardo le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela (*toilette*, stanze d'albergo, cabine, spogliatoi, ecc.). Vanno tenute presenti, inoltre, le norme riguardanti la tutela dei lavoratori, con particolare riferimento alla legge 300/1970 (Statuto dei lavoratori).

Specifici limiti possono derivare da altre speciali disposizioni di legge o di regolamento che prevedono o ipotizzano la possibilità di installare apparecchiature di ripresa locale, aerea o satellitare (d.l. 24 febbraio 2003, n. 28, convertito, con modificazioni, dalla legge 24 aprile 2003, n. 88), disposizioni che, quando sono trattati dati relativi a persone identificate o identificabili, vanno applicate nel rispetto dei principi affermati dal Codice, in tema per esempio di sicurezza presso stadi e impianti sportivi, oppure musei, biblioteche statali e archivi di Stato (d.l. 14 novembre 1992, n. 433, convertito, con modificazioni, dalla legge 14 gennaio 1993, n. 4) e, ancora, relativi a impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali (d.lg. 4 febbraio 2000, n. 45).

Appare inoltre evidente la necessità del rispetto delle norme del codice penale che vietano le intercettazioni di comunicazioni e conversazioni.

2.2. Principio di necessità

Poiché l'installazione di un sistema di videosorveglianza comporta in sostanza l'introduzione di un vincolo per il cittadino, ovvero di una limitazione e comunque di un condizionamento, va applicato il principio di necessità e, quindi, va escluso ogni uso superfluo ed evitati eccessi e ridondanze.

Ciascun sistema informativo e il relativo programma informatico vanno conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (es., programma configurato in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini). Il *software* va configurato anche in modo da cancellare periodicamente e automaticamente i dati eventualmente registrati.

Se non è osservato il principio di necessità riguardante le installazioni delle apparecchiature e l'attività di videosorveglianza non sono lecite *(artt. 3 e 11, comma 1, lett. a), del Codice)*.

2.3. Principio di proporzionalità

Nel commisurare la necessità di un sistema al grado di rischio presente in concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorre un'effettiva esigenza di deterrenza, come quando, ad esempio, le telecamere vengono installate solo per meri fini di apparenza o di "prestigio".

Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi.

Non va adottata la scelta semplicemente meno costosa, o meno complicata, o di più rapida attuazione, che potrebbe non tener conto dell'impatto sui diritti degli altri cittadini o di chi abbia diversi legittimi interessi.

Non risulta di regola giustificata un'attività di sorveglianza rivolta non al controllo di eventi, situazioni e avvenimenti, ma a fini promozionali-turistici o pubblicitari, attraverso *web cam* o *cameras-on-line* che rendano identificabili i

soggetti ripresi.

Anche l'installazione meramente dimostrativa o artefatta di telecamere non funzionanti o per finzione, anche se non comporta trattamento di dati personali, può determinare forme di condizionamento nei movimenti e nei comportamenti delle persone in luoghi pubblici e privati e pertanto può essere legittimamente oggetto di contestazione.

La videosorveglianza è, quindi, lecita solo se è rispettato il c.d. principio di proporzionalità, sia nella scelta se e quali apparecchiature di ripresa installare, sia nelle varie fasi del trattamento *(art. 11, comma 1, lett. d) del Codice)*.

Il principio di proporzionalità consente, ovviamente, margini di libertà nella valutazione da parte del titolare del trattamento, ma non comporta scelte del tutto discrezionali e insindacabili.

Il titolare del trattamento, prima di installare un impianto di videosorveglianza, deve valutare, obiettivamente e con un approccio selettivo, se l'utilizzazione ipotizzata sia in concreto realmente proporzionata agli scopi prefissi e legittimamente perseguibili.

Si evita così un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli altri interessati.

Come si è detto, la proporzionalità va valutata in ogni fase o modalità del trattamento, per esempio quando si deve stabilire:

- se sia sufficiente, ai fini della sicurezza, rilevare immagini che non rendono identificabili i singoli cittadini, anche tramite ingrandimenti;
- se sia realmente essenziale ai fini prefissi raccogliere immagini dettagliate;
- la dislocazione, l'angolo visuale, l'uso di *zoom* automatici e le tipologie - fisse o mobili - delle apparecchiature;
- quali dati rilevare, se registrarli o meno, se avvalersi di una rete di comunicazione o creare una banca di dati, indicizzarla, utilizzare funzioni di fermo-immagine o tecnologie digitali, abbinare altre informazioni o interconnettere il sistema con altri gestiti dallo stesso titolare o da terzi;
- la durata dell'eventuale conservazione (che, comunque, deve essere sempre temporanea).

In applicazione del predetto principio va altresì delimitata rigorosamente:

- anche presso luoghi pubblici o aperti al pubblico, quando sia di legittimo ed effettivo interesse per particolari finalità, la ripresa di luoghi privati o di accessi a edifici;
- l'utilizzazione di specifiche soluzioni quali il collegamento ad appositi "centri" cui inviare segnali di allarme sonoro o visivo, oppure l'adozione di interventi automatici per effetto di meccanismi o sistemi automatizzati d'allarme (chiusura accessi, afflusso di personale di vigilanza, ecc.), tenendo anche conto che in caso di trattamenti volti a definire profili o personalità degli interessati il Codice prevede ulteriori garanzie *(art. 14, comma 1, del Codice)*;
- l'eventuale duplicazione delle immagini registrate;
- la creazione di una banca di dati quando, per le finalità perseguite, è sufficiente installare un sistema a circuito chiuso di sola visione delle immagini, senza registrazione (es. per il monitoraggio del traffico o per il controllo del flusso ad uno sportello pubblico).

2.4. Principio di finalità

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

Si è invece constatato che taluni soggetti pubblici e privati si propongono abusivamente, quale scopo della videosorveglianza, finalità di sicurezza pubblica, prevenzione o accertamento dei reati che invece competono solo ad organi giudiziari o di polizia giudiziaria oppure a forze armate o di polizia.

Sono invece diversi i casi in cui i sistemi di videosorveglianza sono in realtà introdotti come misura complementare volta a migliorare la sicurezza all'interno o all'esterno di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o che hanno lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti.

In ogni caso, possono essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate comunicazioni e/o cartelli di avvertimento al pubblico (fatta salva l'eventuale attività di acquisizione di dati disposta da organi giudiziari o di polizia giudiziaria), e non finalità generiche o indeterminate, tanto più quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti *(art. 11, comma 1, lett. b), del Codice)*. Le finalità così individuate devono essere correttamente riportate nell'informativa.

094

3. ADEMPIMENTI

3.1. Informativa

Gli interessati devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale registrazione; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (concerti, manifestazioni sportive) o di attività pubblicitarie (attraverso *web cam*).

L'informativa deve fornire gli elementi previsti dal Codice *(art. 13)* anche con formule sintetiche, ma chiare e senza ambiguità.

Tuttavia il Garante ha individuato ai sensi dell'art. 13, comma 3, del Codice un modello semplificato di informativa "minima", riportato in fac-simile in allegato al presente provvedimento e che può essere utilizzato in particolare in aree esterne, fuori dei casi di verifica preliminare indicati nel punto successivo. Il modello è ovviamente adattabile a varie circostanze. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, vanno installati più cartelli.

In luoghi diversi dalle aree esterne il modello va integrato con almeno un avviso circostanziato che riporti gli elementi del predetto art. 13 con particolare riguardo alle finalità e all'eventuale conservazione.

Il supporto con l'informativa:

- deve essere collocato nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con la telecamera;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati se le immagini sono solo visionate o anche registrate.

3.2. Prescrizioni specifiche

3.2.1. Verifica preliminare

I trattamenti di dati personali nell'ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti da questa Autorità, anche con un provvedimento generale, come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare *(art. 17 del Codice)*, quando vi sono rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati.

A questo fine, con il presente provvedimento il Garante prescrive a tutti i titolari del trattamento, quale misura opportuna per favorire il rispetto delle previsioni di legge *(art. 143, comma 1, lett. c), del Codice)*, di sottoporre alla verifica preliminare di questa Autorità (anche in tal caso, con eventuali provvedimenti di carattere generale) i sistemi di videosorveglianza che prevedono una raccolta delle immagini collegata e/o incrociata e/o confrontata con altri particolari dati personali (ad es. biometrici), oppure con codici identificativi di carte elettroniche o con dispositivi che rendono identificabile la voce.

La verifica preliminare del Garante occorre anche in caso di digitalizzazione o indicizzazione delle immagini (che rendono possibile una ricerca automatizzata o nominativa) e in caso di videosorveglianza c.d. dinamico-preventiva che non si limiti a riprendere staticamente un luogo, ma rilevi percorsi o caratteristiche fisionomiche (es. riconoscimento facciale) o eventi improvvisi, oppure comportamenti anche non previamente classificati.

3.2.2. Autorizzazioni

I predetti trattamenti devono essere autorizzati preventivamente dal Garante, anche attraverso autorizzazioni generali, quando riguardano dati sensibili o giudiziari, ad esempio in caso di riprese di persone malate o di detenuti *(artt. 26 e 27 del Codice)*.

3.2.3. Altri esami preventivi

Non devono essere sottoposti all'esame preventivo del Garante, a meno che l'Autorità lo abbia disposto, i trattamenti di dati a mezzo videosorveglianza, fuori dei casi indicati nei precedenti punti 3.2.1. e 3.2.2. Non può desumersi alcuna approvazione implicita dal semplice inoltro al Garante di documenti relativi a progetti di videosorveglianza (spesso generici e non valutabili a distanza) cui non segua un esplicito riscontro dell'Autorità, in quanto non si applica il principio del silenzio/assenso.

3.2.4. Notificazione

Gli stessi trattamenti devono essere notificati al Garante solo se rientrano in casi specificamente previsti *(art. 37 del Codice)*. A tale riguardo l'Autorità ha disposto che non vanno comunque notificati i trattamenti relativi a comportamenti illeciti o fraudolenti, quando riguardano immagini o suoni conservati temporaneamente per

esclusive finalità di sicurezza o di tutela delle persone o del patrimonio *(provv. n. 1/2004 del 31 marzo 2004, in G.U. 6 aprile 2004, n. 81 e in www.garanteprivacy.it; v. anche, sullo stesso sito, i chiarimenti forniti con nota n. 9654/33365 del 23 aprile 2004 relativamente alla posizione geografica delle persone).*

3.3. Soggetti preposti e misure di sicurezza

3.3.1. Responsabili e incaricati
Si devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate ad utilizzare gli impianti e, nei casi in cui è indispensabile per gli scopi perseguiti, a visionare le registrazioni *(art. 30 del Codice)*. Deve trattarsi di un numero molto ristretto di soggetti, in particolare quando ci si avvale di una collaborazione esterna.

Vanno osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento, avendo particolare cura al caso in cui il titolare si avvalga di un organismo esterno anche di vigilanza privata *(art. 29 del Codice)*.

La designazione di eventuali responsabili ed incaricati "esterni" può essere effettuata solo se l'organismo esterno svolge prestazioni strumentali e subordinate alle scelte del titolare del trattamento. Questo non deve, ovviamente, essere un espediente per eludere la normativa in materia di protezione dei dati personali, come può accadere, per esempio, nel caso in cui la designazione dell'incaricato *"esterno"* mascheri una comunicazione di dati a terzi senza consenso degli interessati, oppure nel caso di diversità o incompatibilità tra le finalità perseguite dai soggetti che si scambiano i dati.

Quando i dati vengono conservati - naturalmente per un tempo limitato in applicazione del principio di proporzionalità - devono essere previsti diversi livelli di accesso al sistema e di utilizzo delle informazioni, avendo riguardo anche ad eventuali interventi per esigenze di manutenzione. Occorre prevenire possibili abusi attraverso opportune misure basate in particolare su una "doppia chiave" fisica o logica che consentano una immediata ed integrale visione delle immagini solo in caso di necessità (da parte di addetti alla manutenzione o per l'estrazione dei dati ai fini della difesa di un diritto o del riscontro ad una istanza di accesso, oppure per assistere la competente autorità giudiziaria o di polizia giudiziaria). Va infatti tenuto conto che l'accessibilità regolamentata alle immagini registrate da parte degli addetti è fattore di sicurezza.

Sono infine opportune iniziative periodiche di formazione degli incaricati sui doveri, sulle garanzie e sulle responsabilità, sia all'atto dell'introduzione del sistema di videosorveglianza, sia in sede di modifiche delle modalità di utilizzo *(cfr. Allegato B) al Codice, regola n. 19.6)*.

3.3.2. Misure di sicurezza
I dati devono essere protetti da idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta *(art. 31 del Codice)*.

Alcune misure, c.d. "misure minime", sono obbligatorie anche sul piano penale. Il titolare del trattamento che si avvale di un soggetto esterno deve ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle regole in materia *(artt. 33-36 e 169, nonché Allegato B) del Codice, in particolare punto 25; v. anche i chiarimenti forniti con nota n. 6588/31884 del 22 marzo 2004, in www.garanteprivacy.it).*

3.4. Durata dell'eventuale conservazione

In applicazione del principio di proporzionalità *(v. anche art. 11, comma 1, lett. e), del Codice)*, anche l'eventuale conservazione temporanea dei dati deve essere commisurata al grado di indispensabilità e per il solo tempo necessario - e predeterminato - a raggiungere la finalità perseguita.

La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Solo in alcuni specifici casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), è ammesso un tempo più ampio di conservazione dei dati, che non può comunque superare la settimana.

Un eventuale allungamento dei tempi di conservazione deve essere valutato come eccezionale e comunque in relazione alla necessità derivante da un evento già accaduto o realmente incombente, oppure alla necessità di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o di polizia giudiziaria in relazione

ad un'attività investigativa in corso.

Il sistema impiegato deve essere programmato in modo da operare al momento prefissato - ove tecnicamente possibile - la cancellazione automatica da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

3.5. Documentazione delle scelte

Le ragioni delle scelte, cui si è fatto richiamo, devono essere adeguatamente documentate in un atto autonomo conservato presso il titolare e il responsabile del trattamento e ciò anche ai fini dell'eventuale esibizione in occasione di visite ispettive, oppure dell'esercizio dei diritti dell'interessato o di contenzioso.

3.6. Diritti degli interessati

Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Codice, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento e di ottenere l'interruzione di un trattamento illecito, in specie quando non sono adottate idonee misure di sicurezza o il sistema è utilizzato da persone non debitamente autorizzate *(art. 7 del Codice)*.

La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti alla persona istante identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice *(art. 10, commi 3 s., del Codice)*. A tal fine può essere opportuno che la verifica dell'identità del richiedente avvenga mediante esibizione o allegazione di un documento di riconoscimento che evidenzi un'immagine riconoscibile dell'interessato.

4. SETTORI SPECIFICI

4.1. Rapporti di lavoro

Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa e ciò anche in caso di erogazione di servizi per via telematica mediante c.d. "*web contact center*". Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è impiegata per esigenze organizzative e dei processi produttivi, ovvero è richiesta per la sicurezza del lavoro *(art. 4 legge n. 300/1970; art. 2 d.lg. n. 165/2001)*.

Queste garanzie vanno osservate sia all'interno degli edifici, sia in altri luoghi di prestazione di lavoro, così come, ad esempio, si è rilevato in precedenti provvedimenti dell'Autorità a proposito di telecamere installate su autobus (le quali non devono riprendere in modo stabile la postazione di guida, e le cui immagini, raccolte per finalità di sicurezza e di eventuale accertamento di illeciti, non possono essere utilizzate per controlli, anche indiretti, sull'attività lavorativa degli addetti).

È inammissibile l'installazione di sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa (ad es. bagni, spogliatoi, docce, armadietti e luoghi ricreativi).

Eventuali riprese televisive sui luoghi di lavoro per documentare attività od operazioni solo per scopi divulgativi o di comunicazione istituzionale o aziendale, e che vedano coinvolto il personale dipendente, possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica contenute nel Codice, fermi restando, comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico per l'attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine opponendosi anche, per motivi legittimi, alla sua diffusione.

4.2. Ospedali e luoghi di cura

L'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (ad es. unità di rianimazione), stante la natura sensibile di molti dati che possono essere in tal modo raccolti, devono essere limitati ai casi di stretta indispensabilità e circoscrivendo le riprese solo a determinati locali e a precise fasce orarie; devono essere inoltre adottati tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche in attuazione delle doverose misure che il Codice prescrive per le strutture sanitarie *(art. 83)*.

Il titolare deve garantire che possano accedere alle immagini solo i soggetti specificamente autorizzati (es. personale medico ed infermieristico) e che le stesse non possano essere visionate da estranei (ad es. visitatori). Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di familiari di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto.

Le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse, a pena di sanzione penale *(artt. 22, comma 8, e 167 del Codice)*. Va assolutamente evitato il rischio di diffusione delle immagini di persone malate su *monitor* collocati in locali liberamente accessibili al pubblico.

Nei casi in cui l'impiego di un sistema di videosorveglianza all'interno di una struttura sanitaria non sia finalizzato alla cura del paziente, bensì solo a finalità amministrative o di sicurezza (quali, ad esempio, il controllo dell'edificio o di alcuni locali), e sia possibile che attraverso lo stesso siano raccolte immagini idonee a rivelare lo stato di salute, il soggetto pubblico titolare deve menzionare tale trattamento nell'atto regolamentare sui dati sensibili da adottare in base al Codice *(art. 20)*.

4.3. Istituti scolastici

L'eventuale installazione di sistemi di videosorveglianza presso istituti scolastici deve garantire "*il diritto dello studente alla riservatezza*" *(art. 2, comma 2, d.P.R. n. 249/1998)* e tenere conto della delicatezza dell'eventuale trattamento di dati relativi a minori.

A tal fine, se può risultare ammissibile il loro utilizzo in casi di stretta indispensabilità (ad esempio, a causa del protrarsi di atti vandalici), gli stessi devono essere circoscritti alle sole aree interessate ed attivati negli orari di chiusura degli istituti, regolando rigorosamente l'eventuale accesso ai dati.

Restano di competenza dell'autorità giudiziaria o di polizia le iniziative intraprese a fini di tutela dell'ordine pubblico o di individuazione di autori di atti criminali (per es. spacciatori di stupefacenti, adescatori, ecc.).

4.4. Luoghi di culto e di sepoltura

L'installazione di sistemi di videosorveglianza presso chiese o altri luoghi di culto o di ritrovo di fedeli deve essere oggetto di elevate cautele, in funzione dei rischi di un utilizzo discriminatorio delle immagini raccolte e del carattere sensibile delle informazioni relative all'appartenenza ad una determinata confessione religiosa.

Al fine di garantire il rispetto dei luoghi di sepoltura, l'installazione di sistemi di videosorveglianza deve ritenersi ammissibile all'interno di tali aree solo quando si intenda tutelarle dal concreto rischio di atti vandalici.

5. SOGGETTI PUBBLICI

5.1. Svolgimento di funzioni istituzionali

Un soggetto pubblico può effettuare attività di videosorveglianza solo ed esclusivamente per svolgere funzioni istituzionali che deve individuare ed esplicitare con esattezza e di cui sia realmente titolare in base all'ordinamento di riferimento *(art. 18, comma 2, del Codice)*. Diversamente, il trattamento dei dati non è lecito, anche se l'ente designa esponenti delle forze dell'ordine in qualità di responsabili del trattamento, oppure utilizza un collegamento telematico in violazione del Codice *(art. 19, comma 2, del Codice)*.

Tale circostanza si è ad esempio verificata presso alcuni enti locali che dichiarano di perseguire direttamente, in via amministrativa, finalità di prevenzione e accertamento dei reati che competono alle autorità giudiziarie e alle forze di polizia. Vanno richiamate quindi in questa sede le riflessioni già suggerite in passato a proposito di talune ordinanze comunali in tema di prostituzione in luoghi pubblici *(v. provv. 26 ottobre 1998, in Bollettino del Garante n. 6/1998, p. 131)*.

Benché effettuata per la cura di un interesse pubblico, la videosorveglianza deve rispettare i principi già richiamati.

Quando il soggetto è realmente titolare di un compito attribuito dalla legge in materia di sicurezza pubblica o di accertamento, prevenzione e repressione di reati, per procedere ad una videosorveglianza di soggetti identificabili deve ricorrere un'esigenza effettiva e proporzionata di prevenzione o repressione di pericoli concreti e specifici di lesione di un bene (ad esempio, in luoghi esposti a reale rischio o in caso di manifestazioni che siano ragionevolmente fonte di eventi pregiudizievoli).

Non risulta quindi lecito procedere, senza le corrette valutazioni richiamate in premessa, ad una videosorveglianza capillare di intere aree cittadine "cablate", riprese integralmente e costantemente e senza adeguate esigenze. Del pari è vietato il collegamento telematico tra più soggetti, a volte raccordati ad un "centro" elettronico, che possa registrare un numero elevato di dati personali e ricostruire interi percorsi effettuati in un determinato arco di tempo.

Risulta parimenti priva di giustificazione l'installazione di impianti di videosorveglianza al solo fine (come risulta da casi sottoposti al Garante), di controllare il rispetto del divieto di fumare o gettare mozziconi, di calpestare aiuole, di affiggere o di fotografare, o di altri divieti relativi alle modalità nel depositare i sacchetti di immondizia entro gli appositi contenitori.

Le specifiche norme di legge o di regolamento e le funzioni legittimamente individuate dall'ente costituiscono l'ambito operativo entro il quale il trattamento dei dati si intende consentito. Come prescritto dal Codice, l'eventuale comunicazione a terzi è lecita solo se espressamente prevista da una norma di legge o di regolamento *(art. 19, comma 3, del Codice)*.

094

Il Codice individua poi specifiche regole volte invece a consentire, in un quadro di garanzie, riprese audio-video a fini di documentazione dell'attività istituzionale di organi pubblici *(artt. 20-22 e 65 del Codice)*.

Salvo i casi previsti per le professioni sanitarie e gli organismi sanitari, il soggetto pubblico non deve richiedere la manifestazione del consenso degli interessati *(art. 18, comma 4, del Codice)*.

5.2. Informativa

Contrariamente a quanto prospettato da alcuni enti locali, l'informativa agli interessati deve essere fornita nei termini illustrati nel paragrafo 3.1. e non solo mediante pubblicazione sull'albo dell'ente, oppure attraverso una temporanea affissione di manifesti. Tali soluzioni possono concorrere ad assicurare trasparenza in materia, ma non sono di per sé sufficienti per l'informativa che deve aver luogo nei punti e nelle aree in cui si svolge la videosorveglianza.

5.3 Accessi a centri storici

Qualora introducano sistemi di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato, i comuni dovranno rispettare quanto dettato dal d.P.R. 22 giugno 1999, n. 250. Tale normativa impone ai comuni di richiedere una specifica autorizzazione amministrativa, nonché di limitare la raccolta dei dati sugli accessi rilevando le immagini solo in caso di infrazione (*art. 3 d.P.R. n. 250/1999*).

I dati trattati possono essere conservati solo per il periodo necessario per contestare le infrazioni e definire il relativo contenzioso e si può accedere ad essi solo a fini di polizia giudiziaria o di indagine penale.

5.4. Sicurezza nel trasporto urbano

Alcune situazioni di particolare rischio fanno ritenere lecita l'installazione su mezzi di trasporto pubblici di sistemi di videosorveglianza. Tali sistemi di rilevazione sono leciti anche presso talune fermate di mezzi urbani specie in aree periferiche che spesso sono interessate da episodi di criminalità (aggressioni, borseggi, ecc.).

Valgono, anche in questi casi, le considerazioni già espresse a proposito della titolarità in capo alle sole forze di polizia dei compiti di accertamento, prevenzione ed accertamento di reati, nonché del diritto di accesso alle immagini conservate per alcune ore, cui si dovrebbe accedere solo in caso di illeciti compiuti.

Negli stessi casi, deve osservarsi particolare cura anche per ciò che riguarda l'angolo visuale delle apparecchiature di ripresa, nella collocazione di idonee informative a bordo dei veicoli pubblici e nelle aree di fermata - presso cui possono transitare anche soggetti estranei - e per quanto attiene alla ripresa sistematica di dettagli o di particolari non rilevanti riguardanti i passeggeri.

5.5. Deposito dei rifiuti

In applicazione dei principi richiamati, il controllo video di aree abusivamente impiegate come discariche di materiali e di sostanze pericolose è lecito se risultano inefficaci o inattuabili altre misure. Come già osservato, il medesimo controllo non è invece lecito - e va effettuato in altra forma - se è volto ad accertare solo infrazioni amministrative rispetto a disposizioni concernenti modalità e orario di deposito dei rifiuti urbani.

6. PRIVATI ED ENTI PUBBLICI ECONOMICI

6.1. Consenso

A differenza dei soggetti pubblici, i privati e gli enti pubblici economici possono trattare dati personali solo se vi è il consenso preventivo espresso dall'interessato, oppure uno dei presupposti di liceità previsti in alternativa al consenso *(artt. 23 e 24 del Codice)*.

In caso di impiego di strumenti di videosorveglianza da parte di privati ed enti pubblici economici, la possibilità di raccogliere lecitamente il consenso può risultare, in concreto, fortemente limitata dalle caratteristiche e dalle modalità di funzionamento dei sistemi di rilevazione, i quali riguardano spesso una cerchia non circoscritta di persone che non è agevole o non è possibile contattare prima del trattamento. Ciò anche in relazione a finalità (ad es. di sicurezza o di deterrenza) che non si conciliano con richieste di esplicita accettazione da chi intende accedere a determinati luoghi o usufruire di taluni servizi.

Il consenso, oltre alla presenza di un'informativa preventiva e idonea, è valido solo se espresso e documentato per iscritto. Non è pertanto valido un consenso presunto o tacito, oppure manifestato solo per atti o comportamenti concludenti, consistenti ad esempio nell'implicita accettazione delle riprese in conseguenza dell'avvenuto accesso a

094

determinati luoghi.

Nel settore privato, fuori dei casi in cui sia possibile ottenere un esplicito consenso libero, espresso e documentato, vi può essere la necessità di verificare se esista un altro presupposto di liceità utilizzabile in alternativa al consenso, come indicato nel paragrafo successivo.

6.2. Bilanciamento degli interessi

6.2.1. Profili generali
Un'idonea alternativa all'esplicito consenso va ravvisata nell'istituto del bilanciamento di interessi *(art. 24, comma 1, lett. g), del Codice)*. Il presente provvedimento dà attuazione a tale istituto, individuando i casi in cui la rilevazione delle immagini può avvenire senza consenso, qualora, con le modalità stabilite in questo stesso provvedimento, sia effettuata nell'intento di perseguire un legittimo interesse del titolare o di un terzo attraverso mezzi di prova o perseguendo fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, o finalità di prevenzione di incendi o di sicurezza del lavoro.

Considerata l'ampia serie di garanzie e condizioni sopra indicate, non appare necessario che il Garante, per alcuni trattamenti in ambito privato di seguito indicati, prescriva ulteriori condizioni e limiti oltre quelli già richiamati in premessa.

6.2.2. Registrazione delle immagini
I trattamenti di dati possono essere più invasivi rispetto alla semplice rilevazione, qualora siano registrati su supporti oppure abbinati ad altre fonti o conservati in banche di dati, talora solo per effetto di un dispositivo di allarme programmato. E ciò in considerazione delle molteplici attività di elaborazione cui i dati, possono essere sottoposti anche ad altri fini.

In presenza di concrete ed effettive situazioni di rischio tali registrazioni sono consentite a protezione delle persone, della proprietà o del patrimonio aziendale (ad esempio, rispetto a beni già oggetto di ripetuti e gravi illeciti), relativamente all'erogazione di particolari servizi pubblici (si pensi alle varie forme di trasporto) o a specifiche attività (che si svolgono ad esempio in luoghi pubblici o aperti al pubblico, o che comportano la presenza di denaro o beni di valore, o la salvaguardia del segreto aziendale od industriale in relazione a particolari tipi di attività).

6.2.3. Videosorveglianza senza registrazione
Nei casi in cui le immagini sono unicamente visionate in tempo reale, oppure conservate solo per poche ore mediante impianti a circuito chiuso (*Cctv*), possono essere tutelati legittimi interessi rispetto a concrete ed effettive situazioni di pericolo per la sicurezza di persone e beni, anche quando si tratta di esercizi commerciali esposti ai rischi di attività criminali in ragione della detenzione di denaro, valori o altri beni (es., gioiellerie, supermercati, filiali di banche, uffici postali). La videosorveglianza può risultare eccedente e sproporzionata quando sono già adottati altri efficaci dispositivi di controllo o di vigilanza oppure quando vi è la presenza di personale addetto alla protezione.

Nell'uso delle apparecchiature volte a riprendere, per i legittimi interessi indicati, aree esterne ad edifici e immobili (perimetrali, adibite a parcheggi o a carico/scarico merci, accessi, uscite di emergenza), il trattamento deve essere effettuato con modalità tali da limitare l'angolo visuale all'area effettivamente da proteggere, evitando la ripresa di luoghi circostanti e di particolari non rilevanti (vie, edifici, esercizi commerciali, istituzioni ecc.).

6.2.4. Videocitofoni
Sono ammissibili per identificare coloro che si accingono ad entrare in luoghi privati videocitofoni o altre apparecchiature che rilevano immagini o suoni senza registrazione. Tali apparecchiature sono dislocate abitualmente all'ingresso di edifici o immobili in corrispondenza di campanelli o citofoni, appunto per finalità di controllo dei visitatori che si accingono ad entrare. La loro esistenza deve essere conosciuta attraverso una informativa agevolmente rilevabile, quando non sono utilizzati per fini esclusivamente personali *(art. 5, comma 3 del Codice)*.

Altri dispositivi di rilevazione e controllo, invece, spesso non sono facilmente individuabili anche per mancanza di informativa, né la loro collocazione è altrimenti segnalata. In alcuni casi, poi, più telecamere collocate anche all'interno di un edificio (pianerottoli, corridoi, scale) si attivano contemporaneamente e, sia pure per un tempo limitato, riprendono le persone fino all'ingresso negli appartamenti. Anche in questi casi è necessaria una adeguata informativa.

6.2.5. Riprese nelle aree comuni
L'installazione degli strumenti descritti nel paragrafo precedente, se effettuata nei pressi di immobili privati e all'interno di condominii e loro pertinenze (es. posti auto, *box*), benché non sia soggetta al Codice quando i dati non sono comunicati sistematicamente o diffusi, richiede comunque l'adozione di cautele a tutela dei terzi *(art. 5, comma 3, del Codice)*. Al fine di evitare di incorrere nel reato di interferenze illecite nella vita privata *(art. 615-bis c.p.)*, l'angolo visuale delle riprese deve essere limitato ai soli spazi di propria esclusiva pertinenza, ad esempio antistanti l'accesso alla propria abitazione, escludendo ogni forma di ripresa anche senza registrazione di immagini relative ad aree comuni (cortili, pianerottoli, scale, *garage* comuni) o antistanti l'abitazione di altri condomini.

094

Il Codice trova invece applicazione in caso di utilizzazione di un sistema di ripresa di aree condominiali da parte di più proprietari o condomini, oppure da un condominio, dalla relativa amministrazione (comprese le amministrazioni di *residence* o multiproprietà), da studi professionali, società o da enti *no-profit*.

L'installazione di questi impianti è ammissibile esclusivamente in relazione all'esigenza di preservare la sicurezza di persone e la tutela di beni da concrete situazioni di pericolo, di regola costituite da illeciti già verificatisi, oppure nel caso di attività che comportano, ad esempio, la custodia di denaro, valori o altri beni (recupero crediti, commercio di preziosi o di monete aventi valore numismatico).

La valutazione di proporzionalità va effettuata anche nei casi di utilizzazione di sistemi di videosorveglianza che non prevedano la registrazione dei dati, in rapporto ad altre misure già adottate o da adottare (es. sistemi comuni di allarme, blindatura o protezione rinforzata di porte e portoni, cancelli automatici, abilitazione degli accessi).

7. PRESCRIZIONI E SANZIONI

Il Garante invita tutti gli operatori interessati ad attenersi alle prescrizioni illustrate e a quelle definite opportune parimenti indicate nel presente provvedimento, in attesa dei più specifici interventi che potranno derivare in materia da un c.d. provvedimento di verifica preliminare di questa Autorità *(art. 17 del Codice)*, oppure dal codice deontologico che il Garante ha promosso per disciplinare in dettaglio altri aspetti del trattamento dei dati personali effettuato "*con strumenti elettronici di rilevamento di immagini*" *(art. 134 del Codice)*.

Le misure necessarie prescritte con il presente provvedimento devono essere osservate da tutti i titolari di trattamento. In caso contrario il trattamento dei dati è, a seconda dei casi, illecito oppure non corretto, ed espone:

- all'inutilizzabilità dei dati personali trattati in violazione della relativa disciplina *(art. 11, comma 2, del Codice)*;
- all'adozione di provvedimenti di blocco o di divieto del trattamento disposti dal Garante *(art. 143, comma 1, lett. c), del Codice)*, e di analoghe decisioni adottate dall'autorità giudiziaria civile e penale;
- all'applicazione delle pertinenti sanzioni amministrative o penali *(artt. 161 s. del Codice)*.

TUTTO CIÒ PREMESSO IL GARANTE:

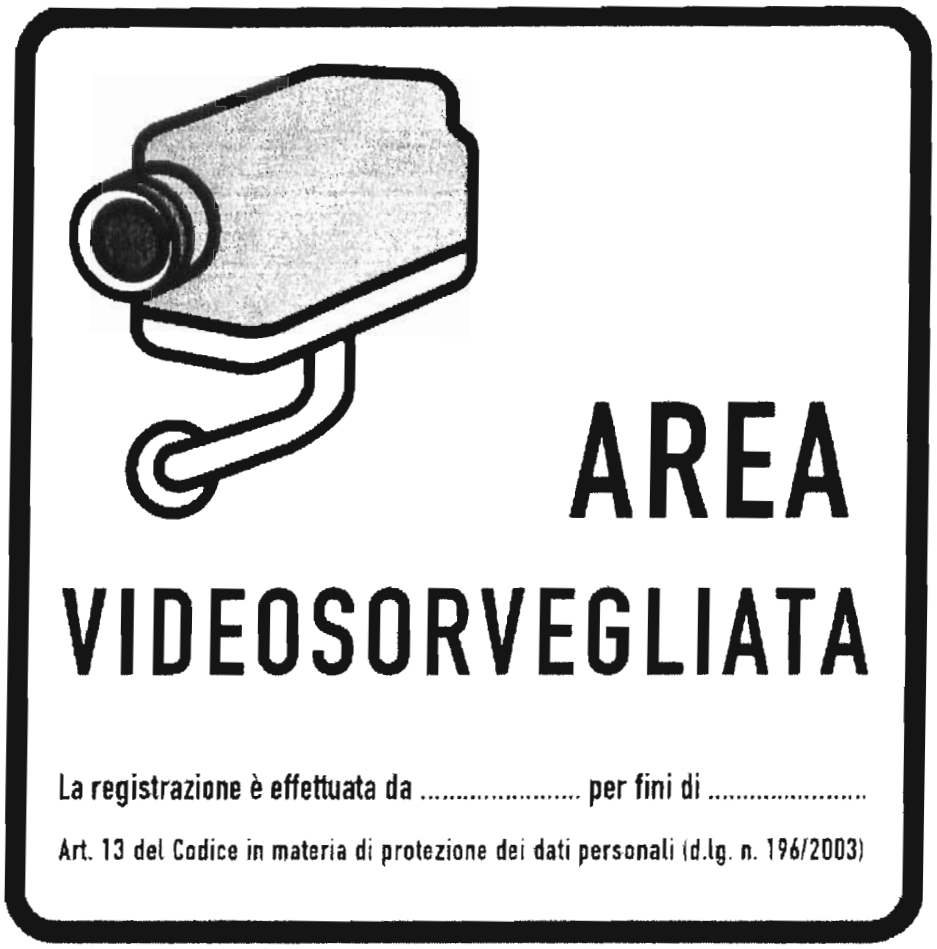
1. prescrive ai titolari del trattamento nei settori interessati, ai sensi dell'art. 154, comma 1, lett. c), del Codice, le misure necessarie ed opportune indicate nel presente provvedimento al fine di rendere il trattamento conforme alle disposizioni vigenti;
2. individua, nei termini di cui in motivazione, ai sensi dell'art. 24, comma 1, lett. f) del Codice, i casi nei quali il trattamento dei dati personali mediante videosorveglianza può essere effettuato da soggetti privati ed enti pubblici economici, nei limiti e alle condizioni indicate, per perseguire legittimi interessi e senza richiedere il consenso degli interessati;
3. individua in allegato un modello semplificato di informativa utilizzabile alle condizioni indicate in motivazione.

Roma, 29 aprile 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli



- Per le modalità di utilizzazione del modello si veda il paragrafo 3.1.
- Se le immagini non sono registrate, sostituire il termine "registrazione" con quello di "rilevazione".

Immagine in formato:

- .EPS
- .JPG
- .GIF

stampa **chiudi**

094

Manuale per la sicurezza ed il corretto trattamento dei dati personali nel Consiglio Nazionale delle Ricerche

(D.lgs. 196/2003)

SOMMARIO

094

PREMESSA

Dal 1° gennaio 2004 è entrato in vigore il Decreto Legislativo 30 giugno 2003 n. 196, noto come Codice in materia di protezione dei dati personali.

Il nuovo codice riunisce in un solo corpus normativo la grande varietà di provvedimenti in materia stratificatisi nel tempo a livello nazionale e comunitario, provvedendo alla loro razionalizzazione e sistematizzazione e migliorando così di molto la fruibilità degli stessi da parte dell'interprete.

Il medesimo inoltre semplifica e snellisce gli adempimenti in precedenza previsti (eliminando molte incombenze a caratteristica prettamente formale) a carico dei titolari del trattamento di dati personali rendendo al tempo stesso tuttavia più stringenti e cogenti i comportamenti e gli obblighi rimasti, al fine di assicurare che la circolazione dei dati e delle informazioni relative alle persone, fisiche e giuridiche, oramai ineliminabile nella odierna società dell'informazione, avvenga nel massimo rispetto dei diritti e delle libertà fondamentali, quali soprattutto il diritto alla riservatezza ed alla identità personale.

E' necessario pertanto che ogni operatore sviluppi sempre più una consapevole cultura circa la "preziosità" e "delicatezza" delle informazioni che quotidianamente è chiamato a trattare e conservare, e che si adoperi affinché vengano compiutamente rispettate, nel suo settore di attività, tutte le misure di sicurezza previste a protezione dei dati stessi, anche per evitare di incorrere nelle pesanti sanzioni, a volte anche di carattere penale, previste dal legislatore a tutela della disciplina di riferimento.

OBBLIGHI DI SICUREZZA

Il diritto alla protezione dei dati personali mira a garantire che il trattamento delle informazioni si svolga "nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali" (art. 1 TU).

Il principio guida dell'azione amministrativa in questo settore è rappresentato pertanto dal "principio di necessità del trattamento", il quale, assieme ai correlati principi di "pertinenza e non eccedenza" , rappresenta un presupposto di liceità del trattamento medesimo.

I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Nell'ambito del predetto obbligo generale di contenere nella misura più ampia possibile determinai rischi, i titolari del trattamento sono tenuti in ogni caso ad assicurare un livello minimo di protezione dei dati mediante l'adozione delle "misure minime di sicurezza" individuate nel Titolo V, Capi I e II del Codice.

SCOPO DEL MANUALE

Nell'ottica di un efficace tutela delle informazioni e dei dati personali gestiti dal CNR, il presente Manuale per la Sicurezza ha lo scopo di fornire le prescrizioni e le istruzioni di massima circa il complesso delle misure organizzative, logistiche, tecniche, ed informatiche da adottare in tutte le strutture, affinché il livello di protezione dei dati personali oggetto di trattamento sia il più possibile conforme a quanto previsto, nel quadro dei più generali obblighi di sicurezza, dal Codice in materia di protezione dei dati personali, e sia tale in ogni caso da garantire il livello minimo di sicurezza previsto dal legislatore.

DEFINIZIONI NORMATIVE

Ai sensi di quanto previsto dal Codice si intende per:

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

dati personali: qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

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

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

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

diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

TRATTAMENTO DI DATI PERSONALI DA PARTE DELLE PUBBLICHE AMMINISTRAZIONI

Alle **Pubbliche Amministrazioni** è consentito:

a) **il trattamento di dati comuni** (diversi da quelli sensibili e giudiziari) se necessario per il perseguimento dei fini istituzionali.

Salvo quanto previsto per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici (parte II del Codice), le PA non devono pertanto acquisire il consenso dell'interessato.

E' tuttavia necessario fornire agli interessati una adeguata **informativa,** in cui si specifichino finalità e modalità del trattamento dei dati, l'eventuale obbligatorietà del loro conferimento, le conseguenze relative la rifiuto di fornire i dati, i diritti esercitabili dall'interessato, nonché i dati identificativi del titolare e del responsabile.

b) **il trattamento dei dati sensibili e giudiziari** se autorizzato da espressa disposizione di legge nella quale si specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

Nei casi in cui una disposizione di legge specifichi le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, le amministrazioni sono tenute ad adottare un apposito regolamento con il quale identificare e rendere pubblici i tipi di dati utilizzabili e le operazioni eseguibili, in relazione ai fini istituzionali perseguiti e nel rispetto dei principi affermati dal Codice.

In ogni caso, il trattamento dei dati sensibili e giudiziari da parte delle Pubbliche Amministrazioni è retto dal principio di indispensabilità, ossia possono essere trattati soltanto i dati sensibili e giudiziari indispensabili allo svolgimento di funzioni istituzionali che non potrebbero essere adempiute altrimenti (mediante il ricorso a dati anonimi o personali di diversa natura).

c) **la comunicazione di dati personali**

- a privati o enti pubblici economici soltanto se prevista da una norma di legge o di regolamento
- ad altri soggetti pubblici se prevista da una norma di legge o di regolamento ovvero, in mancanza, se necessaria per il perseguimento dei fini istituzionali previa apposita comunicazione al Garante per la protezione dei dati personali. Non è in ogni caso consentita la diffusione dei dati idonei a rilevare lo stato di salute.

PROFILI ORGANIZZATIVI

TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

A termini di normativa è titolare del trattamento dei dati personali il soggetto (fisico o giuridico) cui competono, nell'ambito del trattamento medesimo, le decisioni in ordine alle finalità, alle modalità del trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

L'art. 28 del Codice precisa inoltre che, nel caso di trattamento effettuato da una pubblica amministrazione, titolare del trattamento è l'entità nel suo complesso.

Pertanto **titolare del trattamento dei dati effettuato nell'ambito di questo Consiglio è il CNR, nella persona del suo legale rappresentante pro tempore, il Presidente.**

RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI E RELATIVI COMPITI

Sono responsabili del trattamento, ai sensi di quanto disposto dal vigente Regolamento di organizzazione e funzionamento del Consiglio Nazionale delle Ricerche i , **i responsabili pro-tempore delle strutture amministrative, scientifiche e di servizio in cui si articola il CNR, con riferimento ai dati trattati nell'ambito delle Unità Organizzative (comunque denominate) alla cui direzione gli stessi sono preposti.**

Le Unità organizzative di riferimento sono:

- per l'Amministrazione centrale: Uffici delle Direzioni Centrali ed altre eventuali Unità Organizzative specificatamente individuate in quanto non incardinate negli Uffici;
- i Dipartimenti;
- gli Istituti
- le Aree della Ricerca

La nomina a responsabile è effettuata, in sede di prima applicazione della normativa di riferimento, con apposito provvedimento.

A regime, la nomina a responsabile del trattamento dei dati personali sarà contestuale al decreto (o altro provvedimento) di nomina alla direzione della struttura.

L'ambito di responsabilità si estende al trattamento dei dati effettuati, sia con l'ausilio di strumenti elettronici che in maniera cartacea, nell'ambito dell'Unità Organizzativa alla cui direzione il soggetto è preposto, e si riferisce alle tipologie di dati e di trattamenti indicati dal responsabile medesimo nell'apposita scheda di rilevazione fornita, in sede di prima applicazione, in risposta alla circolare pos. 6.9 prot. 0032307 del 16 Giugno 2005, e, successivamente indicati nella costituenda anagrafe elettronica dei trattamenti.

Il CNR si riserva di effettuare, comunque, ulteriori nomine di responsabili, laddove si rendesse necessario, per lo svolgimento di attività istituzionali, delegare a soggetti terzi esterni al CNR il trattamento di alcuni dati.

Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare e contenute nel presente Manuale (e nei successivi aggiornamenti).

Sono compiti del responsabile del trattamento:

- assicurarsi che nell'Unità Organizzativa vengano rispettate le misure minime di sicurezza previste dalla normativa vigente, nonché le altre misure di sicurezza previste dal CNR e riassunte nel presente Manuale.
  Per l'attuazione delle misure di sicurezza in ciascuna unità organizzativa è assicurato il supporto per quanto riguarda il trattamento dei dati, dell'Ufficio Sistemi Informativi, e per quanto riguarda le misure di sicurezza della rete dell'Ufficio Reti e Telecomunicazioni.
  E' possibile contattare i soggetti di riferimento indicati alla pagina web www.cnr.it
  Per il supporto circa l'adozione di misure di sicurezza che non rivestano carattere informatico è possibile contattare l'Ufficio IV della Direzione Generale.

- procedere all'aggiornamento dell'"anagrafe elettronica dei trattamenti dei dati personali" ogni qualvolta si verifichi l'esistenza di un nuovo trattamento, la cessazione di uno precedente, la modifica delle caratteristiche di un trattamento, ovvero il nuovo ingresso, la cessazione o il cambiamento di mansioni di uno degli incaricati.
  L'aggiornamento dell'anagrafe, nella parte relativa ai soggetti incaricati, assolve gli obblighi previsti dalla normativa relativamente all'individuazione scritta del personale incaricato che afferisce (personale tecnico-amministrativo o ricercatore) o risulta assegnato (personale a contratto) alla struttura.
  Qualora il responsabile, nello svolgimento delle sue funzioni istituzionali, ritenga necessario autorizzare soggetti diversi dai precedenti al trattamento dei dati personali inerenti la sua struttura, dovrà provvedere a designare individualmente per iscritto i medesimi(Allegato A).

- comunicare al competente Ufficio dell'Amministrazione Centrale l'eventuale "esternalizzazione" (affidamento all'esterno) di trattamenti di dati personali al fine della predisposizione della nomina a responsabili di tali soggetti.
- comunicare al competente Ufficio dell'Amministrazione Centrale ogni comunicazione di dati personali ad altri soggetti pubblici, effettuata in qualsiasi modo anche tramite convenzione, non prevista da norme di legge o di regolamento ai fini delle necessarie comunicazioni in merito al Garante

- procedere alla richiesta di rilascio e revoca delle autorizzazioni all'accesso a banche dati elettroniche automatizzate.
  Per le banche dati dell'Amministrazione centrale è necessario provvedere ad inoltrare la richiesta al competente Ufficio, il quale poi inoltrerà la stessa al competente personale informatico.

- impartire istruzioni agli incaricati circa il corretto trattamento dei dati personali, dando idonea divulgazione presso gli stessi del presente Manuale per la sicurezza, con particolare riferimento all'appendice relativa alle istruzioni operative per gli incaricati.

- dare idonea diffusione presso i soggetti impegnati in attività di ricerca del "Codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici", affinché le attività medesime siano svolte nel rispetto dei principi e con l'osservanza dei criteri ivi indicati.

- fornire, al momento dell'acquisizione dei dati, per il tramite degli incaricati, ovvero mediante affissione nei locali aperti al pubblico o ancora mediante l'inserimento in moduli o formulari, l'informativa di cui all'art. 13 del Codice agli interessati (Allegato B) .

Il modello di informativa allegato contiene le informazioni generali ed essenziali valide per tutti i trattamenti effettuati all'interno del CNR.

Il suddetto dovrà pertanto essere opportunamente integrato qualora la specificità dei trattamenti effettuati nella singola struttura renda necessarie ulteriori precisazioni.

- evadere, le eventuali domande di accesso, rettifica, integrazione, cancellazione e blocco su istanza degli interessati al trattamento dei dati personali ai sensi degli artt. 7-10 del Codice, previa consultazione, ove lo si ritenga necessario, con l'ufficio competente in materia di disciplina circa il trattamento dei dati personali (Ufficio Sistemi Informativi)
- vigilare affinché l'accesso ai dati da trattare da parte degli incaricati sia limitato a quello strettamente necessari allo svolgimento delle mansioni loro assegnate.

INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

Ai sensi di quanto disposto dalla normativa, gli incaricati del trattamento dei dati personali sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

La designazione va effettuata per iscritto e deve individuare puntualmente l'ambito del trattamento consentito.

Si considera tale tuttavia anche la documentata preposizione della persona fisica all'Unità Organizzativa per la quale è stato individuato per iscritto, l'ambito del trattamento consentito agli addetti della medesima.

Nell'ambito del CNR si considera documentata preposizione l'indicazione degli incaricati preposti ad ogni specifico trattamento all'interno delle schede di rilevazione dei trattamenti inviate in risposta alla circolare n.4/05 del 16 Giugno 2005, ovvero, a regime, indicati nell'anagrafe elettronica dei trattamenti.

Si considerano incaricati pertanto nell'ambito del CNR il personale di ruolo (personale tecnico-amministrativo e ricercatore,) e personale operante ad altro titolo (personale a contratto , dottorandi, titolari di assegni di ricerca) nell'Unità Organizzativa medesima, sulla base di provvedimento o atto formale.

Qualora il responsabile, nello svolgimento delle sue funzioni istituzionali, ritenga necessario autorizzare soggetti diversi dai precedenti al trattamento dei dati personali inerenti la sua struttura, dovrà provvedere a designare per iscritto i medesimi consegnando agli stessi il modello di nomina (ALLEGATO)

Oltre che alle prescrizioni ed istruzioni di carattere generale contenute nel presente Manuale ogni incaricato deve attenersi alle istruzioni impartite dal responsabile dell'Unità Organizzativa cui afferisce od è assegnato relativamente alla specificità del trattamento dei dati personali effettuato nell'Unità Organizzativa medesima.

ANAGRAFE DEL TRATTAMENTO DEI DATI PERSONALI

L'anagrafe elettronica dei trattamenti dei dati personali, contiene i dati relativi alle tipologie ed alle caratteristiche di tutti i trattamenti svolti all'interno del CNR, così come comunicati dalle strutture in risposta alla circolare n.4/05 del 16 Giugno 2005 relativa al censimento generale dei trattamenti.

L'anagrafe costituisce l'unico riferimento circa i trattamenti svolti nel CNR ed i relativi incaricati.

La stessa è implementata e/o modificata, da parte di ciascuna struttura, ogni qualvolta si verifichi l'esistenza di un nuovo trattamento, la cessazione di uno precedente, la modifica delle caratteristiche di un trattamento, ovvero il nuovo ingresso, la cessazione o il cambiamento di mansioni di uno degli incaricati.

LA SICUREZZA

Nell'ambito informatico, comunemente, il termine "sicurezza" si riferisce a tre aspetti distinti:

Riservatezza: Prevenzione contro l'accesso non autorizzato alle informazioni;

Integrità: Le informazioni non devono essere alterabili da incidenti o abusi;

Disponibilità Il sistema deve essere protetto da interruzioni impreviste.

Il TU sulla privacy pone una particolare attenzione, agli articoli 31 e seguenti, alle tematiche della sicurezza dei dati e sistemi.

In proposito le misure di sicurezza da adottare vengono distinte in:

- misure idonee e preventive volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
- misure minime, indicate negli articoli 34 e 35 e analiticamente specificate nel Disciplinare Tecnico e diversificate a seconda che il trattamento sia effettuato o meno con strumenti elettronici.

Con l'approvazione del Codice i titolari di trattamento di dati (quindi anche il CNR) sono tenuti ad **adottare, quanto meno, le cd "misure minime di sicurezza"**, ossia gli accorgimenti, individuati negli artt. 34-35 e nel Disciplinare Tecnico del Codice, tesi ad assicurare un livello minimo di protezione dei dati personali.

La mancata osservanza di quanto stabilito in materia di misure minime di sicurezza e sanzionata penalmente (arresto fino a due anni o ammenda da diecimila a cinquantamila euro).

L'adozione delle misure minime di sicurezza non esonera tuttavia da responsabilità civile qualora l'eventuale danneggiato dimostri che, in base all'evoluzione tecnologica raggiunta, era possibile e raccomandabile l'utilizzo di misure di sicurezza ulteriori (le cd misure "idonee").

Per l'attuazione delle misure di sicurezza in ciascuna unità organizzativa è assicurato il supporto dell'Ufficio Sistemi Informativi.

Saranno concordati, presso ciascuna struttura, appositi incontri con personale tecnico - informatico, al fine di evidenziare eventuali criticità e predisporre un piano di adeguamento.

Per il supporto circa l'adozione di misure di sicurezza che non rivestano carattere informatico è assicurato il supporto dell'Ufficio .IV della Direzione Generale.

LE MISURE MINIME DI SICUREZZA

- **Trattamenti effettuati con strumenti elettronici**

Trattamento dati comuni

Sono **obbligatorie** le seguenti misure:

a) autenticazione informatica.
Il sistema informatico deve essere dotato di mezzi (le cd. credenziali di autenticazione) deputati alla verifica ed alla convalidazione dell'identità del soggetto che vi accede Le credenziali di autenticazione consistono in un codice per l'identificazione (user id) dell'incaricato associato a una parola chiave riservata (password), conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave..

b) adozione di procedure di gestione delle credenziali di autenticazione;
Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali

c) utilizzazione di un sistema di autorizzazione;
E' il sistema che, dopo l'autenticazione, permette agli incaricati di trattare effettivamente i dati.
I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
E' effettuata tramite l'aggiornamento, almeno annuale, dell'anagrafe del trattamento dei dati personali.

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
Utilizzo di antivirus aggiornati almeno *semestralmente* (giornalmente) e adozione di *misure atte alla protezione dagli accessi dalla rete (firewall etc)*

094

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
Utilizzo di back up e strategie di disaster recovery

g) tenuta di un aggiornato documento programmatico sulla sicurezza (redatto annualmente dal CNR).

Trattamento dati sensibili o giudiziari

Ulteriori misure:

h) Adozione di idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni

i) Devono essere concordate con l'Ufficio Sistemi Informativi le misure organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

- **Trattamenti effettuati senza l'ausilio di strumenti elettronici (dati su supporto cartaceo)**

Trattamento dati comuni

Sono **obbligatorie** le seguenti misure:

a) L'aggiornamento periodico dei dati il cui trattamento è consentito agli incaricati (tramite l'aggiornamento dell'anagrafe dei trattamenti)

b) Istruzioni circa un'idonea custodia degli atti e dei documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

E' compito di ciascun responsabile fornire istruzioni agli incaricati del trattamento affinché ai documenti contenenti dati personali non accedano persone prive di autorizzazione, dando idonea divulgazione presso gli stessi del presente Manuale per la sicurezza, per quanto riguarda le prescrizioni di carattere generale, nonché impartendo le istruzioni del caso relativamente alla specificità del trattamento dei dati personali effettuato nell'Unità Organizzativa medesima.

Trattamento dati sensibili o giudiziari

Ulteriori misure:

L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, possibilmente utilizzando armadi o contenitori chiusi a chiave

Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori dall'orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

094

APPENDICE

ISTRUZIONI OPERATIVE PER GLI INCARICATI

A) Trattamenti senza l'ausilio di strumenti elettronici

1. UTILIZZATE LE CHIAVI!

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio quando l'ultima unità di personale lascia il locale e, comunque, alla fine della giornata e chiudete i documenti a chiave negli armadi ogni volta che potete.

2. NON COMUNICATE DATI PERSONALI A SOGGETTI NON LEGITTIMATI

L'utilizzo dei dati personali deve avvenire in base al cd "principio di necessità", è cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative.

I dati non devono essere comunicati all'esterno del CNR e comunque a soggetti terzi, se non previa autorizzazione del Responsabile nelle ipotesi consentite dalla normativa vigente.

3. FATE ATTENZIONE A COME DISTRUGGETE I DOCUMENTI

Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

I documenti originali non possono in alcun caso essere distrutti senza la previa autorizzazione della Soprintendenza Archivistica.

4. RADDOPPIATE LE ATTENZIONI SE I DOCUMENTI CONTENGONO DATI SENSIBILI O GIUDIZIARI

I documenti contenenti dati sensibili e/o giudiziari devono essere controllati e custoditi
molto attentamente in modo che non vi accedano persone prive di autorizzazione.

Ad esempio, la consultazione di documenti o certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattia, ecc., deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati.

L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando possibilmente armadi o contenitori chiusi a chiave

Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori dall'orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

Riponete i documente contenenti dati sensibili o giudiziari negli appositi contenitori o scaffali al termine delle operazioni affidate e comunque a fine giornata.

In ogni caso di allontanamento dal proprio posto di lavoro, documenti devono essere riposti negli armadi o nei cassetti, possibilmente chiusi a chiave.

B) Trattamenti con strumenti elettronici

1. **CONSERVATE I DISCHETTI (FLOPPY DISK) OVVERO I COMPACT DISC IN UN LUOGO SICURO**
   Per i dischetti e i compact disc si applicano gli stessi criteri che per i documenti cartacei. Riponeteli negli armadi o nei cassetti non appena avete finito di usarli.

2. **UTILIZZATE LE PASSWORD**
   Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:
   a) La password di accesso al computer impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.
   b) La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.
   c) La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
   d) La password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.

   Imparate a utilizzare questi quattro tipi fondamentali di password, e mantenete distinta almeno quella di tipo *a*, che può dover essere resa nota, almeno temporaneamente, esclusivamente ai tecnici accreditati incaricati dell'assistenza. Scegliete le password secondo le indicazioni della sezione successiva.

3. **ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI**
   Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe.

4. **PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI**
   I PC portatili sono un facile bersaglio per i furti. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup periodico.

5. **NON FATEVI SBIRCIARE QUANDO STATE DIGITANDO LE PASSWORD**
   Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.

6. **CUSTODITE LE PASSWORD IN UN LUOGO SICURO**
   Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

7. **NON UTILIZZATE APPARECCHI NON AUTORIZZATI**
   L'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete, ed è quindi vietata. Per l'utilizzo di altri apparecchi, consultatevi con l'Ufficio Sistemi Informativi.

8. **NON INSTALLATE PROGRAMMI NON AUTORIZZATI**
   Solo i programmi istituzionali o acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con l'Ufficio Sistemi Informativi.

9. **APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS**
   La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

Linee guida per la prevenzione dei virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

COME SI TRASMETTE UN VIRUS:

1. Attraverso programmi provenienti da fonti non ufficiali;
2. Attraverso le macro dei programmi di automazione d'ufficio.

COME *NON* SI TRASMETTE UN VIRUS:

1. Attraverso file di dati non in grado di contenere macro (file di testo, html, pdf, ecc.);
2. Attraverso mail non contenenti allegati.

QUANDO IL RISCHIO DA VIRUS SI FA SERIO:

1. Quando si installano programmi;
2. Quando si copiano dati da dischetti;
3. Quando si scaricano dati o programmi da Internet.

QUALI EFFETTI HA UN VIRUS?

1. Effetti sonori e messaggi sconosciuti appaiono sul video;
2. Nei menù appaiono funzioni extra finora non disponibili;
3. Lo spazio disco residuo si riduce inspiegabilmente;

COME PREVENIRE I VIRUS:

1. **USATE SOLTANTO PROGRAMMI PROVENIENTI DA FONTI FIDATE**
   Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati.

2. **ASSICURATEVI DI NON FAR PARTIRE ACCIDENTALMENTE IL VOSTRO COMPUTER DA DISCHETTO**
   Infatti se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files.

3. **PROTEGGETE I VOSTRI DISCHETTI (O COMPACT DISK) DA SCRITTURA QUANDO POSSIBILE**
   In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

4. **ASSICURATEVI CHE IL VOSTRO SOFTWARE ANTIVIRUS SIA AGGIORNATO**
   La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Informatevi con l'Ufficio Sistemi Informativi per maggiori dettagli.

5. **NON DIFFONDETE MESSAGGI DI PROVENIENZA DUBBIA**
   Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignoratelo: i mail di questo tipo sono detti con terminologia anglosassone *hoax* (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete.

6. **NON PARTECIPATE A "CATENE DI S. ANTONIO" E SIMILI**
   Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono *hoax*, aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche.

SCELTA DELLE PASSWORD

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

COSA NON FARE

1. NON dite a nessuno la Vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome
2. NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
3. Quando immettete la password NON fate sbirciare a nessuno quello che state battendo sulla tastiera.
4. NON usate il Vostro nome utente. È la password più semplice da indovinare
5. NON usate password che possano in qualche modo essere legate a Voi come, ad esempio, il Vostro nome, quello di Vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

COSA FARE

1. Cambiare la password a intervalli regolari.
2. Usare password lunghe almeno otto caratteri con un misto di lettere, numeri e segni di interpunzione.

ALLEGATO A

Al Dott./Sig.

OGGETTO: incaricato per il trattamento dei dati personali (art. 30 D.lvo 196/2003)

Il/la sottoscritto/a , in qualità di responsabile della struttura del CNR di seguito specificata:

TIPOLOGIA	DENOMINAZIONE
Amministrazione centrale	
Struttura scientifica	

nominato/a dal titolare quale responsabile del trattamento di dati personali svolto presso la struttura di riferimento

autorizza

il/la Sig./a ,
al trattamento delle seguenti tipologie di dati personali, limitatamente al tempo di vigenza del rapporto in essere con il CNR

.....
contenuti in atti e documenti redatti su supporto cartaceo ovvero nella banca dati di seguito indicata (eventuale)

.....

Al riguardo il dott/sig si impegna ad effettuare il trattamento dei dati di competenza osservando le seguenti istruzioni:

a) Il nominato svolgerà il predetto incarico attenendosi ai criteri previsti dalla normativa vigente sulla tutela dei dati personali e sulle misure di sicurezza relative, anche con riferimento ai regolamenti ed alle modalità tecniche adottate dal CNR, riferiti sia al trattamento di dati personali riguardanti archivi di tipo cartaceo o effettuati con strumenti automatizzati diversi da quelli elettronici, sia relativi al trattamento di dati personali effettuato con strumenti automatizzati elettronici.
A questo proposito prenderà opportuna conoscenza di quanto previsto nel "Manuale per la sicurezza ed il corretto trattamento dei dati personali nel Consiglio Nazionale delle Ricerche".

b) Il nominato, qualora impegnato in attività di ricerca, si atterrà ai principi ed ai criteri indicati nel "Codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici ".

b) Il nominato si asterrà dal compiere attività di trattamento che comportino un accesso ed una conoscenza di informazioni superiore rispetto all'ambito di trattamento dei dati attribuitogli.

c) Il nominato incaricato è tenuto a tutelare la conservazione e l'integrità dei dati personali affidatigli per il trattamento.

Il Responsabile del trattamento
L'incaricato

Sede della Struttura li,

094

ALLEGATO B

Informativa ai sensi dell'art.13 del Decreto Legislativo 30 giugno 2003, n.196 – Codice in materia di protezione dei dati personali

Ai sensi del Decreto Legislativo 30 giugno 2003 n.196 - *Codice in materia di protezione dei dati personali*, che prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, di seguito definito "codice", si informa su quanto segue:

1. TRATTAMENTO DEI DATI

Per trattamento si intende qualunque operazione o complesso di operazioni effettuate, anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati personali, anche se non registrati in una banca dati.

2. FINALITA' DEL TRATTAMENTO DEI DATI

Il trattamento dei dati personali è finalizzato all'espletamento da parte del CNR, delle funzioni istituzionali e dei compiti previsti dalla legge, dai regolamenti o dalla normativa comunitaria, nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza.
La normativa contenuta nel codice prevede che il CNR, come ogni altro Ente Pubblico, provveda, nell'ambito dello svolgimento delle funzioni istituzionali, al trattamento dei dati personali, senza la necessità di chiedere il consenso dell'interessato.
Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal codice, anche in relazione alla diversa natura dei dati medesimi.

3. MODALITA' DEL TRATTAMENTO

I dati personali oggetto di trattamento sono:

a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi;
c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

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

4. CONFERIMENTO DEI DATI

Il conferimento dei dati, in quanto trattati soltanto al fine di adempiere le funzioni istituzionali del CNR, è obbligatorio.
L'eventuale rifiuto al conferimento determina, pertanto, l'impossibilità da parte dell'Amministrazione ad adempiere alle proprie funzioni istituzionali e quindi l'impossibilità per l'interessato di beneficiare degli eventuali servizi e/o prestazioni richiesti.

5. SOGGETTI DESTINATARI DELLA COMUNICAZIONE E DIFFUSIONE DEI DATI

Qualora sia previsto da una disposizione di legge o di regolamento ovvero sia necessario per l'adempimento delle funzioni istituzionali i dati personali trattati dal CNR possono essere comunicati ad altri soggetti pubblici. La comunicazione di dati a soggetti privati è effettuata esclusivamente qualora prevista da una norma di legge o di regolamento.

6. DIRITTI DELL'INTERESSATO

L'interessato ha diritto:

a) di conoscere l'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e alla loro comunicazione in forma intelligibile;
b) di essere informato dal titolare circa le finalità del trattamento;
c) di ottenere dal titolare la conferma, l'aggiornamento, l'integrazione ovvero la rettifica dei propri dati;
d) di ottenere la cancellazione, la trasformazione in forma anonima ovvero il blocco dei dati trattati in violazione di legge;
e) di opporsi in tutto o in parte, per motivi legittimi, al trattamento di dati che lo riguardano;

Tali diritti sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato.
L'interessato, in caso di mancata soddisfazione della richiesta da parte dei suddetti soggetti, può far valere i propri diritti adendo l'Autorità giudiziaria ovvero tramite ricorso al Garante.

7. TITOLARE E RESPONSABILE DEL TRATTAMENTO DEI DATI

Titolare del trattamento dei dati è il Consiglio Nazionale delle Ricerche in persona del suo legale rappresentante pro-tempore, e per esso del Direttore Generale ai sensi del provvedimento del Presidente del CNR n.54 del 1 luglio 2005, domiciliato per la carica presso la sede del CNR in P.le Aldo Moro, 7 Roma.
Responsabili del trattamento dei dati sono i Responsabili pro-tempore delle strutture amministrative, di ricerca e di servizio in cui si articola il CNR (per l'Amministrazione centrale: i Dirigenti.)