

LEGGE 675/96 - LA PROTEZIONE DEI DATI PERSONALI

Si riportano, nelle pagine che seguono, alcuni degli schemi di sintesi proposti e commentati nel corso del Seminario condotto dall'Ing. ADALBERTO BIASIOTTI (Securcomp S.r.l.)

REGISTRAZIONI AUDIO

COSA SI DEVE FARE

- se l'ordine (di mediazione) è impartito telefonicamente, deve essere registrato su nastro magnetico od altro supporto equivalente (*Regolamento CONSOB artt. 11, 29 e 30*)
- deve essere possibile il riascolto a breve
- il supporto deve essere conservato con diligenza per almeno due anni (*Regolamento CONSOB artt. 25 e 35*)

COSA SI PUÒ FARE

- fare copie di sicurezza
- aggiungere alla registrazione, anche in forma automatica, l'identificativo di data/ora

COSA NON SI DEVE FARE

- registrare senza aver informato la controparte
- comunicare il contenuto a terzi non interessati
- custodire con negligenza le registrazioni
- eliminare i supporti prima che una possibile contestazione abbia potuto essere verificata (*registro e trattazione reclami*)
- eliminare i nastri senza averli prima accuratamente cancellati

REGISTRAZIONI VIDEO

COSA SI DEVE FARE

- preavvertire il cliente che si entra in zona di ripresa
- evitare che alcuno esamini le immagini registrate od anche in diretta, se non è stato nominato incaricato del trattamento ex Legge 675/96
- impartire le opportune istruzioni all'incaricato della gestione dei supporti
- custodire con cautele i supporti registrati

COSA SI PUÒ FARE

- fare copie di sicurezza
- esaminare con terzi aventi titolo le registrazioni, ai soli fini di sicurezza, con garanzia di riservatezza

COSA NON SI DEVE FARE

- conservare le registrazioni oltre il tempo utile per lo scopo per cui sono state effettuate (ad esempio, 15 giorni)
- permettere che estranei le osservino
- custodire con negligenza le registrazioni

- eliminare i nastri senza averli prima accuratamente cancellati
- comunicare o diffondere alcuna notizia, desunta dalle registrazioni, non avente cogente giustificazione di sicurezza.

GALATEO E DOVERI TELEFONICI

COSA SI DEVE FARE

- preavvertire il cliente che le sue telefonate potrebbero essere ascoltate abusivamente da terzi estranei, se del caso (D.Lgs. 13 maggio 1998, n. 171 – art. 3, comma 2)
- preavvertire il cliente prima di passare in *viva voce* in presenza di terzi, anche colleghi (D.Lgs. 13 maggio 1998, n. 171 – art. 3, comma 3)
- preavvertire il cliente prima di mettere in ascolto su una derivazione terzi, anche colleghi (D.Lgs. 13 maggio 1998, n. 171 – art. 3, comma 3)

COSA SI PUÒ FARE

- rifiutare di rispondere a chiamanti che abbiano bloccato la identificazione del chiamante, se disponibile (D.Lgs. 13 maggio 1998, n. 171 – art. 6, comma 3)
- bloccare la presentazione identificazione del chiamante (D.Lgs. 13 maggio 1998, n. 171 – art. 6, comma 2)
- bloccare la presentazione della propria identificazione nei confronti del chiamante (D.Lgs. 13 maggio 1998, n. 171 – art. 6, comma 4)
- chiedere la soppressione del blocco della identificazione del chiamante, in caso di molestatori (D.Lgs. 13 maggio 1998, n. 171 – art. 7, comma 1)

COSA NON SI DEVE FARE

- effettuare spedizioni automatiche di fax, senza consenso espresso del chiamato (D.Lgs. 13 maggio 1998, n. 171 – art. 10, comma 1)

REGISTRARE SI, REGISTRARE NO

Dopo le numerose telefonate con minacce di attentati terroristici fatti dall'IRA in Inghilterra, molte aziende, anche su sollecitazione della Polizia, hanno attivato dei dispositivi automatici di registrazione delle chiamate entranti. Per legge questi dispositivi devono emettere ad intervalli regolari un segnale acustico, una sorta di bip, per avvertire il chiamante che la linea è sotto registrazione.

Anche se i giornali non hanno dato ampio risalto a questo fatto, pochi utenti sembrano al corrente della situazione, come dimostra una indagine condotta nel 1993 per conto dell'OFTTEL (office of Telecommunication).

Agli intervistati è stato chiesto se sapevano cosa significhi il bip che veniva udito ad intervalli durante la comunicazione (risposte nella tab. 1). Successivamente, è stato chiesto agli intervistati se dava loro fastidio il fatto che la telefonata fosse registrata (risposte nella tab. 2).

Tab. 1

<i>Interpretazione</i>	<i>% degli intervistati</i>
Guasto sulla linea	17

Tab. 2

<i>Reazione dell'intervistato</i>	<i>% in caso di ascolto</i>	<i>% in caso di registraz.</i>
Molto infastidito	38	48

<i>Chiamata sotto controllo</i>	12
Altra chiamata in attesa	12
Conversazione registrata	3
Linea in prove tecniche	2
Altri	26
Non so	30

<i>Abbastanza infastidito</i>	13	13
Non infastidito	31	25
Dipende dalle circostanze	16	13
Non so	1	1

A questo punto, è stato chiesto quale tra i seguenti mezzi di informazione sarebbe più appropriato onde avvertire il chiamante che la chiamata è registrata. Sono state offerte quattro alternative:

- il centralino telefonico riproduce automaticamente un messaggio prima dell'inoltro della chiamata, ricordando che la conversazione potrebbe essere intercettata o registrata;
- l'azienda fa una dichiarazione relativa al fatto che le informazioni ottenute dall'ascolto delle conversazioni devono essere usate esclusivamente per l'addestramento del personale;
- un breve segnale acustico all'inizio della chiamata indica che essa può essere ascoltata o registrata;
- un breve tono viene trasmesso ogni trenta secondi circa per ricordare al chiamante che la chiamata può essere sotto controllo.

V'è da dire che l'atteggiamento degli intervistati è un poco cambiato dopo che è stato loro spiegato che molto spesso è la Polizia che richiede la registrazione delle chiamate entranti, per disporre di un valido strumento di sussidio all'indagine sugli attentati terroristici.

In altri casi, per contro, le telefonate vengono registrate perché fanno riferimento a transazioni finanziarie, per le quali è necessario poter disporre di una prova certa. Anche in questo caso, la maggioranza degli utenti si è dichiarata contraria alle registrazioni delle telefonate, anche se preavvertiti.

In sintesi, il diritto alla privacy della telefonata sembra ancora essere primario, almeno per i cittadini britannici.

**BOZZA DEL REGOLAMENTO RECANTE NORME IN MATERIA DI
“INDIVIDUAZIONE DELLE MISURE DI SICUREZZA MINIME PER IL
TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL’ARTICOLO 15,
COMMA 2, DELLA LEGGE 31 DICEMBRE 1996, N. 675”.**

**CAPO I
PRINCIPI GENERALI**

**Art. 1
(Definizioni)**

1. Ai fini del presente regolamento si applicano le definizioni elencate nell’articolo 1 della legge 31 dicembre 1996, n. 675, di seguito denominata legge. Ai medesimi fini si intende per “misure minime”, il complesso delle norme tecniche informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall’articolo 15, comma 1, della legge; per “strumenti” si intendono i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento.

**Art. 2
(Elencazione delle misure minime)**

1. Le misure minime, secondo quanto previsto dagli articoli seguenti, riguardano:
 - a) l’identificazione dell’utente;
 - b) l’autorizzazione all’accesso alle funzioni, ai servizi, ai locali, ai dati;
 - c) la registrazione degli ingressi;
 - d) i limiti al riutilizzo di supporti di archiviazione elettronica automatizzata o cartacea.
2. Le misure minime di questo regolamento non si applicano agli elaboratori utilizzati esclusivamente per la fornitura di servizi di inoltro di traffico telematico e non accessibili per altre funzionalità.

**CAPO II
TRATTAMENTO DEI DATI PERSONALI EFFETTUATO
CON STRUMENTI ELETTRONICI E COMUNQUE AUTOMATIZZATI**

**SEZIONE I
TRATTAMENTO DEI DATI PERSONALI EFFETTUATI PER FINI ESCLUSIVAMENTE PERSONALI**

**Art. 3
(Misure minime)**

1. Il trattamento dei dati personali e dei dati sensibili effettuato con elaboratori non accessibili da altri elaboratori e terminali ed utilizzato per fini esclusivamente personali ai sensi dell’articolo 3 della legge è soggetto unicamente all’obbligo di proteggere l’accesso ai dati o all’intero sistema mediante l’utilizzo di una parola chiave.

**SEZIONE II
TRATTAMENTO DEI DATI PERSONALI EFFETTUATO MEDIANTE ELABORATORI NON ACCESSIBILI DA ALTRI
ELABORATORI O TERMINALI**

**Art. 4
(Identificazione degli incaricati)**

1. Se il trattamento dei dati personali è effettuato mediante elaboratori non accessibili da altri elaboratori

o terminali a fini diversi da quelli esclusivamente personali di cui all'articolo 3 della legge, il titolare e, se designato, il responsabile adottano, anteriormente all'inizio del trattamento, le seguenti misure:

- a) prevedere una parola chiave per l'accesso ai dati e fornirla agli incaricati del trattamento. La parola chiave, quando gli incaricati sono più di uno, deve essere distinta per ciascuno di essi;
- b) individuare per iscritto, quando gli incaricati del trattamento sono più di uno, i soggetti che hanno accesso alle informazioni relative alle parole chiave e controllare e custodire le informazioni medesime.

SEZIONE III

TRATTAMENTO DEI DATI PERSONALI EFFETTUATO MEDIANTE ELABORATORI ACCESSIBILI IN RETE

Art. 5

(Classificazione)

1. Ai fini della presente sezione gli strumenti [elaboratori accessibili in rete] impiegati nel trattamento dei dati personali sono distinti in
 - a) elaboratori accessibili da altri elaboratori solo attraverso reti non disponibili al pubblico;
 - b) elaboratori accessibili mediante una rete di telecomunicazioni disponibile al pubblico.

Art. 6

(Codici identificativi e protezione degli strumenti)

1. Oltre a quanto previsto dall'articolo 4, nel caso di trattamenti effettuati con gli strumenti di cui all'articolo 5, comma 1, lettere a) e b), devono essere adottate le seguenti misure:
 - a) a ciascun utente o incaricato del trattamento deve essere attribuito un codice identificativo personale. Uno stesso codice non può, neppure in tempi diversi, essere assegnato a persone diverse;
 - b) i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di mancato utilizzo per periodi superiori ai sei mesi;
 - c) le stazioni di lavoro ed i server di rete [, qualora possibile,] devono essere protetti contro il rischio di intrusione ad opera di virus informatici o altri programmi destinati al danneggiamento dei dati o del sistema, mediante idonei programmi aggiornati con cadenza almeno semestrale.

Art. 7

(Documento programmatico sulla sicurezza)

1. Nel caso di trattamento dei dati personali effettuato con gli strumenti di cui all'articolo 5, comma 1, lettere a) e b), questi devono essere inseriti in un inventario periodico redatto con cadenza almeno annuale.
2. Nel caso di trattamento dei dati personali effettuato con gli strumenti indicati nell'articolo 5, comma 1, lettera b) deve essere predisposto o aggiornato con periodicità annuale, un documento programmatico sulla sicurezza dei dati che, sulla base della analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture organizzative preposte al trattamento dei dati stessi, definisce:
 - a) i criteri tecnici ed organizzativi per la protezione delle aree e dei locali rilevanti ai fini delle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
 - b) i criteri e le procedure per assicurare la integrità dei dati;
 - c) i criteri e le procedure per la sicurezza delle trasmissioni dei dati per via telematica;
 - d) la elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni;
3. L'efficacia delle misure di sicurezza adottate ai sensi del comma 2, deve essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale.

Art. 8

(Autorizzazione all'accesso)

1. per il trattamento dei dati sensibili effettuato ai sensi dell'articolo 5, comma 1, lettere a) e b), l'accesso per effettuare le operazioni di trattamento è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione.
2. Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare e, se designato, dal responsabile. Periodicamente, e comunque almeno una volta l'anno, si deve procedere alla verifica della sussistenza delle condizioni per la loro conservazione.
3. L'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.
4. La validità delle richieste di accesso ai dati personali deve essere verificata prima di consentire l'accesso stesso.
5. Non è consentita la utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

Art. 9**(Reimpiego dei supporti di memorizzazione)**

1. Nel caso di trattamento dei dati personali effettuato con gli strumenti di cui all'articolo 5, comma 1, lettere a) e b), i supporti già utilizzati per l'archiviazione dei dati sensibili non possono essere riutilizzati qualora le informazioni precedentemente contenute siano recuperabili e devono essere distrutti.
2. Gli insiemi temporanei di dati devono essere interamente eliminati al termine della procedura che li ha generati.

CAPO III**TRATTAMENTO DEI DATI PERSONALI EFFETTUATO
CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI****Art. 10****(Trattamento di dati personali)**

1. Nel caso di trattamento di dati personali effettuato con strumenti diversi da quelli previsti dal capo II, sono osservate le seguenti modalità:
 - a) gli incaricati devono essere preventivamente autorizzati per iscritto ad accedere ai dati in misura strettamente connessa con le necessità del trattamento delegato;
 - b) i dati devono essere conservati in archivi non accessibili a chiunque e, se consegnati al personale addetto al trattamento, devono essere da quest'ultimo conservati e restituiti al termine del trattamento.

Art. 11**(Trattamento di dati sensibili)**

1. Nel caso di trattamento di dati sensibili effettuato con strumenti diversi da quelli previsti dal capo II, sono osservate le seguenti modalità:
 - a) gli incaricati devono essere preventivamente autorizzati per iscritto ad accedere ai dati sensibili in misura strettamente connessa con le necessità del trattamento delegato;
 - b) i dati devono essere conservati in archivi accessibili al solo personale incaricato della conservazione e, se consegnati al personale addetto al trattamento, devono essere da quest'ultimo conservati in contenitori muniti di serratura;
 - c) l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.

Art. 12

(Conservazione della documentazione relativa al trattamento)

1. I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali sensibili devono essere conservati e custoditi con le modalità di cui agli articoli 10 e 11. Se la documentazione non è più necessaria per le finalità del trattamento, e non costituisce originale da conservare per periodi diversi ai sensi delle norme vigenti, deve essere distrutta non oltre sessanta giorni dalla conclusione del trattamento.