# 23. GLI ADEMPIMENTI DEI PROVIDER

## GLI OBBLIGHI DEL PROVIDER

Il Provider è titolare del trattamento dei dati relativi ai propri clienti/utenti ed alle attività da essi svolte; soggiace quindi alle norme del Codice o di altre leggi sulla privacy (e di un eventuale futuro codice deontologico). In particolare e ad esemplificazione, è tenuto al rispetto delle norme riguardanti:

- ***Modalità di trattamento dei dati e loro requisiti (art. 11)***

I dati debbono essere:
- trattati in modo lecito e secondo correttezza;
- esatti ed aggiornati;
- pertinenti (non eccedenti alle finalità per cui sono raccolti);
- conservati in modo che sia identificabile l'interessato per il tempo strettamente necessario a conseguire le finalità per cui sono raccolti;
- raccolti e registrati per fini determinati, espliciti, legittimi e compatibili con quelli dichiarati.

- ***Informativa (art. 13)***

- Va resa prima di procedere alla raccolta dei dati.
- E' necessaria anche quando c'è l'esonero dal consenso.
- Va resa anche via Internet qualora si proceda alla raccolta dei dati necessari per la conclusione del contratto.
- Va collocata prima della richiesta di registrazione virtuale dei dati.

A carico del Provider è prevista anche l'informativa (art. 131) sulla sussistenza di situazioni che possono permettere ad estranei di apprendere i contenuti di comunicazioni o conversazioni (anche abbonati ed utenti debbono darsi tale informazione e sulla possibilità che ciò dipenda dal tipo di terminale o di collegamento utilizzato dall'utente).

- ***Consenso (art. 23)***

Non necessario per adempiere ad obblighi contrattuali o precontrattuali (art. 24.1, lett. b).
E' quindi necessario:
- quando ci siano dati "non necessari" alla stipula o esecuzione del contratto;
- quando i dati siano raccolti per finalità diverse dalla stipula o esecuzione del contratto.

Si ritiene valido il consenso prestato via e-mail o via web.
Sempre necessario se si trattano dati sensibili. Un consenso valido è prestato dall'interessato solo con firma digitale.

- ***Notificazione***

E' necessaria solo nel caso che i trattamenti effettuati rientrino nell'ipotesi dell'art. 37, comma 1, lett d ("dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti").

- ***Misure di sicurezza***

- Art. 31: misure di sicurezza "idonee" a ridurre al minimo i rischi
  - di distruzione o perdita, anche accidentale, dei dati;
  - di accesso non autorizzato;
  - di trattamento non consentito o non conforme alle finalità della raccolta.

In particolare al provider, è richiesta (art. 32, comma 1):
  - la sicurezza dei servizi;
  - l'integrità dei dati relativi al traffico, all'ubicazione e alla comunicazione, rispetto ad ogni forma di utilizzazione o conoscenza non consentita.
- Artt. 33/36 + Allegato B
  La mancata adozione delle "misure minime" previste comporta sanzione penale; l'adozione non esclude la responsabilità civile, se non si rivelano "idonee" ad escludere il rischio

## LE SCANSIONI DEL PROVIDER ANTI VIRUS E SPAM

La meritoria attività dei provider, volta a ridurre prassi dannose ed intromissioni nelle comunicazioni elettroniche, individuando virus (anche senza il consenso dell'utente), messaggi spam (così permettendo all'utente di disattivare appositi filtri) e specifici contenuti illeciti (che richiederebbero il consenso o l'intervento dell'autorità giudiziaria), può tradursi anche in una interferenza nelle libertà di comunicazione. Merita quindi di essere riportato il "Parere 2/2006 – 21.2.06" (newsletter 7.3.2006) del gruppo dei Garanti europei, mirante a fornire indicazioni per lo svolgimento di tale attività.
I Garanti europei invitano anzitutto i provider ed i produttori di software ad "incorporare i principi di tutela della privacy nei programmi utilizzati per la gestione della posta elettronica, riducendo al minimo il trattamento dei dati personali".
Il parere si sofferma poi sulle attività di:

- ***Scansione ai fini di individuare virus***

Rientra tra gli obblighi di sicurezza imposti dalla Direttiva 2002/58 e non è necessario il consenso dell'utente. Il provider ha tuttavia l'obbligo: di informare l'utente sulla natura dell'attività svolta (es.: nelle condizioni contrattuali del servizio); non rivelare ad alcuno il contenuto della comunicazione. Se la ricerca del virus comporta la scansione dei contenuti dei messaggi l'analisi va limitata esclusivamente alla ricerca dei possibili virus.

- ***Screening per individuare spam***

Anche questa può configurarsi come misura di sicurezza a tutela della funzionalità del servizio di posta elettronica, ma contro il pericolo di filtrare messaggi che non sono spam (con conseguente limitazione della libertà di comunicazione) l'utente deve essere posto in grado di disapplicare i filtri e stabilire quali tipi di spam siano filtrati.

I Garanti invitano i provider ed i produttori di software e di programmi di posta elettronica a creare strumenti che permettano all'utente di configurare in modo autonomo i meccanismi di filtraggio.

- ***Scansione per la ricerca di contenuti potenzialmente illeciti***

E' una vera intercettazione della comunicazione, che può essere effettuata solo dall'autorità giudiziaria e dalle forze di polizia. Non rientra negli obblighi standard dei provider ma può essere offerta come "servizio a valore aggiunto", che richiede espresso consenso dell'utente interessato al controllo.

**BANCHE DATI DEI PROVIDER**

- ***Elenco degli abbonati***

  Una specie di elenco degli abbonati (dati anagrafici e username).

  Generalmente accessibile al pubblico

- ***Archivio della password***

  cioè delle chiavi private che, in combinazione con l'username, consentono l'accesso al sistema. Non aperto al pubblico. Misure elevate di sicurezza

- ***Archivio dei log (Registro dei DATA LOG)***

  cioè delle registrazioni automatiche delle transizioni e dei collegamenti.

  E' il Provider che decide quali informazioni registrare (essenziali: per pure finalità tariffarie; complesse: mappa precisa e dettagliata delle connessioni, con chi, per quanto tempo).

  Il Codice deontologico dell'ANFOV (Associazione nazionale fornitori di audio-video informazioni) stabilisce che debba contenere le informazioni per risalire a:

  - l'identità dell'interessato che accede al sistema o alla rete telematica , in via temporanea o permanente:
  - l'identità dell'interessato che ha utilizzato il servizio per diffondere o distribuire contenuti.

Aspetti rilevanti per i data log:

- divieto di utilizzo delle informazioni per fini non concordati o non consentiti (es.: profilazione dell'utente);
- diritto d'accesso dell'interessato;
- accesso dell'autorità giudiziaria per l'accertamento dei reati;
- informativa sui contenuti dei log, sempre dovuta all'interessato;
- consenso sempre necessario per i dati sensibili; per i dati comuni è escluso solo per finalità contrattuali e d'esecuzione.

- ***Problemi d'attenzione per i provider***

- *il flusso dei dati:*
  a) in Europa;
  b) in USA (aderenti/non aderenti al "Privacy Shield");
  c) in altri Paesi (contratti tipo).
- *lo spamming*

con Codice e Garante che privilegiano l'*opt in.*

- *la separazione di responsabilità*

  c'è la tendenza ad escludere il provider dalla responsabilità dei dati contenuti nelle transazioni (responsabilità dell'utente); controversa è invece la sua responsabilità quando gestisce gruppi di discussione virtuale.

Opportunità pratiche:

a) indicare con chiarezza le regole di comportamento;
b) verificare regolarmente i contenuti presenti;
c) eliminare i contenuti illeciti**.**

## TEMPI DI CONSERVAZIONE DEI DATI TELEFONICI E TELEMATICI

### ***Le disposizioni legislative***

La conservazione dei dati di traffico è facoltativa o obbligatoria, rispettivamente in base agli articoli 123 e 132 del Codice della privacy.

**Art. 123** – Conservazione per finalità contrattuali e commerciali.

Premesso il principio che vanno cancellati o resi anonimi i dati quando non sono più necessari ai fini della comunicazione elettronica, l'art. 123 consente la conservazione dei dati di traffico, sia telefonico che telematico, per 6 mesi (salva ulteriore durata per

contestazione, anche giudiziale) per esigenze di documentazione in caso di contestazione della fattura o di pretesa di pagamento.

E' consentita anche la conservazione per la durata necessaria ai fini della commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi di valore aggiunto, purché vi sia il preventivo consenso dell'abbonato/utente (revocabile in ogni momento).

Il trattamento dei dati è consentito solo agli "incaricati" (art. 30) che attendono a tali attività, che debbono essere identificabili nei loro accessi.

**Art. 132** – Conservazione per finalità di accertamento e repressione reati.

Originariamente l'obbligo di conservazione era limitato ai dati di traffico telefonico.

Il c.d. "pacchetto Pisanu" (art. 6 D.L. 27.7.05, n. 144, conv. con mod. dalla L. 31.7.05, n. 155) ha imposto lunghi tempi di conservazione dei dati di traffico, sia telefonici che telematici, motivandoli con la finalità dell'accertamento e repressione dei reati, e (modificando l'art. 132) ne stabiliva la durata:

A) in 2 anni per i dati di traffico telefonico (anche relativi a telefonate senza risposta) e in 6 mesi per quelli telematici, al fine dell'accertamento e repressione dei reati;
B) in ulteriori 2 anni (dati telefonici) e 6 mesi (dati telematici) per l'accertamento e la repressione dei delitti in danno dei sistemi informatici e telematici o di quelli per i quali l'art. 407, comma 2, lett. a) del c.p.p. prevede l'arresto in flagranza. In sede penale i dati potevano essere conservati anche oltre questo periodo se il giudice riteneva sussistessero "sufficienti" indizi di questi tipi di delitto.

A "regime transitorio" veniva poi prescritto il divieto di cancellazione dei dati di entrambi i tipi di traffico fino al 31.12.07, termine poi prorogato al 31.12.08 (D.L. 31.12.07, n. 248, conv. in L. 27.2.08, n. 31).

I tempi di conservazione così fissati erano considerati tra i più lunghi d'Europa (es.: in Finlandia la conservazione era sui 3 mesi) e andavano oltre i tempi massimi previsti dalla Direttiva 2006/24/CE (c.d. "direttiva Frattini"), con la quale l'U.E. ha cercato di raggiungere una certa uniformità tra i vari paesi.

Il D.Lgs. 30.5.2008, n. 109 (Gazzetta Ufficiale, Serie Generale, n. 141 del 18.6.08) recependo la Direttiva e ad essa adeguandosi e conseguentemente modificando l'art. 132 del Codice privacy:

- elimina ogni distinzione in base al tipo di reato;
- mantiene inalterati i tempi di conservazione dei dati telematici (6mesi + 6 mesi);
- riduce a 2 anni la conservazione dei dati telefonici (a soli 30 giorni i dati per le telefonate senza risposta);
- col 1° comma dell'art. 5 introduce nel Codice della privacy un art. 162 bis che, per violazione delle disposizioni di cui all'art. 132, comma 1-1bis, stabilisce una sanzione amministrativa (da 10.000 a 50.000 Euro) triplicabile[1] in ragione delle condizioni economiche del contravventore;

[1] Ora quadruplicabile in forza dell'art. 164 bis del Codice.

- col 2° comma sempre dell'art. 5, stabilisce una sanzione pecuniaria:
- da 10.000 a 50.000 Euro per l'omesso o incompleta conservazione dei dati prevista dall'art. 132, comma 1-1bis;
- da 5.000 a 50.000 Euro per l'assegnazione di un indirizzo IP che non consenta l'identificazione univoca dell'utente o abbonato.

In entrambi i casi la sanzione è triplicabile in ragione delle condizioni economiche del contravventore. La violazione è contestata e la sanzione è applicata dal Ministero per lo sviluppo economico.

Le categorie di dati telefonici e telematici da conservare, sono dettagliatamente elencate nell'art. 3 del decreto legislativo.

Con D.L. 2.10.08, n. 151 (convertito con modifiche dalla L. 28.11.08, n. 186) sono state praticamente bloccate le norme di recepimento della direttiva comunitaria (D.Lgs. n. 109/08) fino al 31 marzo 2009, ripristinando per lo stesso tempo il "pacchetto Pisanu" e quindi permettendo ai gestori

- di non cancellare i dati con conservazione scaduta, o che verranno a scadenza;
- di registrare i dati senza tener conto delle categorie indicate dall'art. 3 del D. Lgs. n. 109/08, compresi quelli delle telefonate senza risposta;
- di assegnare gli indirizzi IP anche se non consentono l'identificazione dell'utente o dell'abbonato.

DISPOSIZIONI INTRODOTTE IN MATERIA DI ANTITERRORISMO

Per quanto l'Art. 4-bis del decreto legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, come modificato dal decreto legge 30 dicembre 2015, n. 210, convertito con modificazioni dalla legge 25 febbraio 2016, n. 21, non costituisca una vera e propria modifica al regime di conservazione dei dati di traffico e telematici quanto piuttosto una previsione in deroga, riguardando unicamente i reati in materia di terrorismo previsti dal Codice di procedura penale, è innegabile sia consigliata una sua conoscenza. Il testo dell'art. 4-bis è il seguente:

"1. I dati relativi al traffico telefonico o telematico, esclusi comunque i contenuti di comunicazione, detenuti dagli operatori dei servizi di telecomunicazione alla data di entrata in vigore della legge di conversione del presente decreto, nonché quelli relativi al traffico telefonico o telematico effettuato successivamente a tale data, sono conservati, *in deroga a quanto stabilito dall'articolo 132, comma 1, del codice di cui al decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni*, fino al 30 giugno 2017, per le finalità di accertamento e di repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale.

2. I dati relativi alle chiamate senza risposta, effettuate a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica

accessibile al pubblico oppure di una rete pubblica di comunicazione, sono conservati fino al 30 giugno 2017.

3. Le disposizioni di cui ai commi 1 e 2 cessano di applicarsi a decorrere dal 1° luglio 2017".

## ***Le disposizioni del Garante***

Va premesso che i "dati relativi al traffico telematico" si riferiscono solo alle caratteristiche esteriori (conversazione, chiamata, comunicazione), con divieto assoluto di desumere i contenuti; i fornitori sono quindi tenuti a conservare solo i dati di traffico che hanno disponibili in quanto strumentali per rendere il servizio offerto (numero chiamato, data, ora, durata; localizzazione del chiamante con cellulare; indirizzi e-mail contattati, data, ora, durata degli accessi alla Rete).

Il comma 5 dell'art. 132 del Codice della privacy stabilisce che il trattamento dei dati di traffico nella conservazione sopra indicata debba avvenire nel rispetto delle misure e degli accorgimenti dettati dal Garante (a norma dell'art. 17); questi era intervenuto più volte in materia e, con deliberazione del 19 settembre 2007, adottava il documento "Misure e accorgimenti a garanzia degli interessati in tema di conservazione di traffico telefonico e telematico per finalità di accertamento e repressione dei reati"; sul documento avviava anche una consultazione pubblica, a conclusione della quale, tenendo conto dei commenti e delle osservazioni pervenuti e delle risultanze dei diversi incontri, a livello sia tecnico che associativo, emanava il provvedimento generale "Sicurezza dei dati di traffico telefonico e telematico – 17 gennaio 2008" (modificato con Provvedimento 24 luglio 2008).

Numerose sono le prescrizioni impartite nel provvedimento; di seguito succinte e significative esemplificazioni.

- Acquisizione dei dati conservati per accertamento e repressione dei reati.

Questi dati si possono acquisire solo per tali specifiche finalità, quindi il gestore non deve fornirli per controversie civili, amministrative e contabili.

Entro i tempi di conservazione dell'art. 132 si può accedere ai dati con decreto motivato del P.M., anche su istanza del difensore dell'imputato, della persona indagata, della persona offesa e delle altre parti private.

- Accesso ai locali

I locali che ospitano i sistemi di elaborazione dei dati di traffico per sole finalità di giustizia debbono disporre di sistemi biometrici di controllo degli accessi.

- Accesso ai dati

L'accesso è consentito solo al personale incaricato mediante strumenti avanzati (strong autentication) di autenticazione informatica, anche con l'uso di dati biometrici (es.: impronta digitale).

Ciò vale anche per gli incaricati di mansioni tecniche ed anche per gli amministratori di sistema (figura questa per la quale il Garante si era riservato approfondimento ed ulteriore provvedimento).

- Sistemi di autorizzazione

Vanno separati i compiti di chi accede ai dati da quelli di chi assegna le credenziali di autenticazione. Nei profili di autorizzazione debbono essere differenziati gli incaricati che attendono all'ordinaria gestione, da quelli che attendono ai dati di traffico conservati per l'accertamento e repressione dei reati.

- Tracciamento dell'attività degli incaricati

In apposito "audit log" vanno registrati tutti gli accessi e tutte le operazioni compiuti dagli incaricati e dagli amministratori di sistema.

- Conservazione separata

I dati conservati per esclusive finalità di accertamento/repressione reati vanno trattati con sistemi informativi distinti fisicamente da quelli utilizzati per altre gestioni aziendali (fatturazione, antifrode, marketing) e vanno protetti con idonei strumenti di protezione perimetrale a salvaguardia delle reti di comunicazione e delle risorse di memorizzazione impiegate.

- Cancellazione dei dati

Scaduti i termini di conservazione i dati vanno subito cancellati o resi anonimi anche dalle copie di backup.

- Controlli interni

Vanno effettuati controlli periodici su: legittimità degli accessi da parte degli incaricati; rispetto delle norme di legge; adozione delle misure organizzative e di sicurezza prescritte dal Garante; effettiva cancellazione dei dati allo scadere dei termini di conservazione.

- Sistemi di cifratura

Per evitare i rischi di acquisizione indebita (anche fortuita) di informazioni registrate, da parte di affidatari di mansioni tecniche (amministratori di sistema, manutentori hardware e software) i dati di traffico per accertamento e repressione dei reati vanno protetti con tecniche crittografiche.

I gestori avrebbero dovuto adeguarsi alle prescrizione del provvedimento del Garante entro il 30 aprile 2009 (entro il 30.6.2009 per dotarsi di *strong autentication*); accogliendo la richiesta di Assitel, fondata sulla complessità degli adempimenti, con provvedimento del 29 aprile 2009 (G.U. 11.5.09, n. 107) l'Authority ha prorogato entrambi i termini al 15 dicembre 2009.
Infine va precisato che il provvedimento, sia per evitare inutili accumuli di dati, sia perché trattasi di soggetti non assimilabili a veri e propri gestori, non trova applicazione nei confronti di: gestori di esercizi pubblici e Internet cafè, gestori di siti Internet che diffondono contenuti sulla rete (content provider), gestori di motori di ricerca, pubbliche amministrazioni che mettono a disposizione del personale reti telefoniche ed informatiche (es.: centralini aziendali) o che si avvalgono di server messi a disposizione da altri soggetti.

## CONSERVAZIONE DATI PER PICCOLI PROVIDER

Accogliendo le istanze di Assoprovider il Garante ha ritenuto accettabile (newsletter n. 339 del 24.6.2010) una soluzione associativa per una sicura conservazione dei dati di traffico telematico e telefonico da parte dei piccoli provider. Questi, riuniti in gruppo, potranno affidare ad uno di loro o ad una società esterna la realizzazione e la gestione della piattaforma di conservazione dei dati di traffico; ognuno di essi avrà credenziali differenziate per accedere al proprio spazio di memoria all'interno del server centralizzato. La memorizzazione dei dati dovrà avvenire in forma criptata la cui chiave di decodifica è tenuta dal solo singolo provider e l'amministratore del sistema non potrà accedere ai contenuti dei file archiviati. Scaduti i termini di conservazione i dati di traffico dovranno essere cancellati automaticamente.

## MAGGIORE TUTELA NEL SETTORE DELLE COMUNICAZIONI ELETTRONICHE[2]

Al recepimento della Direttiva 2009/136/CE nel settore delle comunicazioni elettroniche si è provveduto col D. Lgs. 28 maggio 2012, n. 69, che ha modificato ed integrato diversi articoli del Codice della privacy ed ha imposto nuovi oneri per i fornitori di servizi di comunicazione elettronica accessibile al pubblico.

- Modifiche e integrazioni alle definizioni dell'art. 4, comma 2, del Codice
  - lett. a) ed f) = la parola "abbonato" è sostituita dalla parola "contraente";
  - lett. b) = è così sostituita la definizione di "chiamata": "la connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale";
  - lett. c) = "reti di comunicazione elettronica": i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato";
  - lett. d) una "rete pubblica di comunicazioni" è ora così definita. "una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di rete";
  - lett. i) = la definizione di "dati relativi all'ubicazione" è così sostituita: "ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica

[2] Le nuove disposizioni non riguardano i gestori di siti internet che diffondono contenuti sulla Rete (content provider) e i gestori di motori di ricerca.

dell'apparecchiatura terminale dell'utente di un servizio di comunicazione accessibile al pubblico".

- lett. g-bis) = lettera aggiunta che così definisce la violazione dei dati personali: "violazione della sicurezza che comporta anche accidentalmente la distinzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto di forniture di un servizio di comunicazione accessibile al pubblico".

- Obblighi e adempimenti a carico dei fornitori dei servizi.

  Particolarmente significativi appaiono gli articoli 32 (sostituito anche nella titolazione) e 32 bis (aggiunto interamente):

  - "Art. 32 - Obblighi relativi ai fornitori di servizi di comunicazione elettronica accessibili al pubblico».

    Il fornitore deve adottare (anche attraverso altri soggetti cui affidi l'erogazione del servizio) le misure tecniche ed organizzative adeguate al rischio esistente, a salvaguardia delle sicurezza dei suoi servizi. Va garantita la protezione dei dati relativi al traffico, all'ubicazione, agli altri dati archiviati o trasmessi, contro i rischi: di distruzione (anche accidentale), perdita o alterazione; di trattamento, accesso, divulgazione non autorizzati o illeciti.

    I dati personali debbono essere accessibili "soltanto al personale autorizzato per fini legalmente autorizzati".

  - "Art. 32-bis – Adempimenti conseguenti ad una violazione di dati personali".

    Il fornitore, in caso di "violazione dei dati personali" (così come definita) deve darne comunicazione – senza indugi – al Garante; anche al contraente, o altra persona, se la violazione può arrecare pregiudizio ai loro dati personali o alla loro riservatezza. Questa ultima comunicazione non è dovuta se il fornitore dimostra al Garante che tecnicamente aveva reso i dati inintelligibili.

    La comunicazione al Garante deve contenere le misure proposte o adottate per porre rimedio; la comunicazione al contraente deve contenere maggiori informazioni (natura della violazione, punti di contatto per maggiori spiegazioni, misure raccomandate per ridurre i possibili effetti pregiudiziali).

    Il Garante può emanare, con proprio provvedimento, orientamenti ed istruzioni sul come assolvere l'obbligo della comunicazione.

Sono sorti dubbi sull'applicabilità della disciplina tlc anche alle persone giuridiche, scomparse dalla definizione di "dati personali", ma è prevalsa l'opinione che anche le persone giuridiche, enti, associazioni ne siano tutelati guardando alla definizione di contraente [art. 4.2, lett. f) introdotta al D.Lgs. 69/2012] che invece li comprende[3].

Si sostiene tuttavia la necessità di un ulteriore ritocco legislativo perché l'art. 121 stabilisce che le disposizioni del Titolo X del Codice privacy ("comunicazioni

3 Ved. Circolare n. 23 del 3.9.2012 di Assonime.

elettroniche") "si applicano al trattamento dei dati personali" (che per l'art. 4.1 non sono riferibili che alle persone fisiche.

## DATA BREACH - LINEE GUIDA DEL GARANTE

In attuazione dell'art. 32-bis del già citato D.Lgs. n. 69/2012 e dopo consultazione pubblica, il Garante ha adottato il "Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) - 4 aprile 2013" (G.U. – Serie generale n. 97 del 26.4.2013).

Il Provvedimento pone l'obbligo per società telefoniche ed internet provider[4] di comunicare all'Authority le violazioni di dati personali (data breach) contenuti in data base elettronici o cartacei.

Sono esclusi dall'obbligo: i siti internet che diffondono contenuti, i motori di ricerca, gli internet point, le reti aziendali; le banche dati che non attengono in maniera specifica al servizi offerto (es.: gestione del personale, contabilità).

Entro 24 ore dalla scoperta dell'evento i soggetti tenuti alla comunicazione dovranno fornire all'Authority tutte le informazioni necessarie (es.: tipologia dei dati coinvolti, descrizione dei sistemi di elaborazione, indicazione del luogo della violazione) per una prima valutazione dell'entità della violazione attraverso un modello disponibile sul sito (www.garanteprivacy.it).

Nei casi più gravi di violazione, entro tre giorni, dovranno essere informati anche tutti gli utenti coinvolti dalla violazione sul grado di pregiudizio che la perdita o la distruzione dei dati può comportare e sull'attualità, qualità e quantità dei dati coinvolti.

La comunicazione agli utenti non è dovuta se si dimostra di aver utilizzato misure di sicurezza e sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati.

Le società telefoniche e i provider dovranno tenere un inventario costantemente aggiornato (violazioni subite, circostanze in cui queste si sono verificate, conseguenze, provvedimenti adottati a seguito del loro verificarsi).

Sono previste sanzioni amministrative per:

• mancata o ritardata comunicazione al Garante (da 25 mila a 150 mila euro);

• omessa o mancata comunicazione agli utenti (da 150 a 1000 euro per ogni società, ente o persona interessata);

• mancata tenuta dell'inventario aggiornato (da 20 mila a 120 mila euro).

## DISCIPLINA DEI COOKIES

Il D.lgs. n. 69/2012 è intervenuto in materia modificando interamente l'articolo 122 del Codice, così adeguandosi alla Direttiva 2009/136/CE che vede nell'apparecchiatura

[4] La disciplina del data breach è stata estesa anche ad altre tipologie di soggetti e di violazioni riguardanti, ad esempio, sistemi biometrici (Provv. n. 513 del 12.11.2014), dossier sanitario elettronico tenuto da strutture pubbliche e private (Provv. n. 331 del 4.6.2015), alle amministrazioni pubbliche (Provv. n. 392

terminale di un utente e nelle informazioni in essa contenuta una sfera privata da tutelare contro ogni intrusione di terzi.

I cookies costituiscono archiviazione di informazioni sull'apparecchiatura di un utente o accesso a informazioni già archiviate, per diverse finalità che possono essere lecite (snellimento dei collegamenti; carrello di spesa) o illecite (intrusione di software spia; virus). Il nuovo art. 122 prescrive che l'utente/contraente, previa chiara informativa, consenta espressamente l'archiviazione o l'accesso (salvo che nella misura strettamente necessaria al fornitore per erogare un servizio esplicitamente richiesto dal contraente/utente).

Ai fini dell'espressione del consenso possono essere utilizzate specifiche configurazioni di programmi/dispositivi informatici di facile e chiara utilizzabilità (ma nulla appare sul come rendere l'informativa all'utente).

Per fornire chiare regole operative sull'uso dei cookies il Garante ha avviato una consultazione pubblica, rivolta ai gestori dei siti e alle associazioni dei consumatori; la consultazione si è conclusa il 19 marzo 2013 ma è solo l'8 maggio 2014 che adotta il Provvedimento "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie" (G.U. 3.6.204, n. 126)[5].

I titolari dei siti web hanno avuto tempo fino al 2 giugno 2015 per adeguarsi alle disposizioni del provvedimento di seguito succintamente richiamato.

Nel Provvedimento il Garante ha stabilito che si blocchi l'installazione dei cookie ai fini di profilazione e marketing da parte dei gestori di siti senza che questi abbiano prima reso l'informativa on line (appositamente semplificata) agli utenti sull'uso dei cookie e abbiano acquisito il loro consenso libero e consapevole.

Quando si accede alla home page o ad un'altra pagina di un sito web deve immediatamente comparire un banner (ne ha predisposto anche un modello esemplificativo) ben visibile, in cui sia indicato chiaramente:

- che il sito utilizza cookie di profilazione prima parte per inviare pubblicità mirata in linea con le preferenze manifestate dall'utente nell'ambito della navigazione;
- che il sito consente anche l'invio di cookie di terze parti (cookie installati da un sito diverso tramite il sito che si sta visitando) di profilazione o analitici per i quali non sono stati adottati strumenti volti a ridurre il potere identificativo dei dati trasmessi dei cybernauti;
- un link a una informativa più ampia, contenete le indicazioni sull'uso dei cookie inviati dal sito, dove è possibile negare il consenso alla loro installazione direttamente o collegandosi ad altri siti nel caso dei cookie di "terze parti";
- l'indicazione che proseguendo nella navigazione (ad es., accedendo ad un'altra area del sito o selezionando un'immagine o un link) si presta il consenso all'uso dei cookie.

Il Garante ha anche predisposto il seguente fac-simile:

[5] Vista la complessità del tema al Provvedimento del 2014 sono seguiti numerosi altri interventi da parte dell'Authority quali: le FAQ del 3.12.2014, il tutorial del 15.1.2015, la scheda informativa del 5.6.2015, le infografiche del 10.6.2015 e del 22.7.2015.


- *Tipologie di cookies*

  Vengono individuate due macro categorie di cookie:

  *a) cookie tecnici*

  Normalmente installati dal titolare o dal gestore (possono essere di navigazione o di sessione) e garantiscono la navigazione e la fruizione del sito web (permettendo di realizzare un acquisto o l'autenticazione per accedere ad aree riservate)

  Sono assimilabili i «*cookie analitici di prima parte*» (se realizzati e utilizzati direttamente dal gestore del sito per raccogliere informazioni, in forma aggregata, ad esempio sul numero degli utenti e su come questi visitano il sito stesso) e i «cookie di funzionalità», che permettono all'utente la navigazione in funzione di una serie di criteri selezionati (es.: lingua, i prodotti selezionati per l'acquisto) al fine di migliorare il servizio reso allo stesso.

  Non è richiesto il consenso; il gestore del sito deve fornire solo l'informativa che ritiene più idonea.

  Per i cookie analitici di terze parti, invece, occorre fare un distinguo:

  - se vengono adottati strumenti idonei a ridurne il potere identificativo, ad esempio mascherando porzioni significative dell'indirizzo IP, può essere fornita l'informativa ritenuta più ideona;
  - se non vengono adottati strumenti idonei a ridurne il potere identificativo occorre quantomeno inserire il banner.

  *b) cookie di profilazione*

Sono volti a creare profili relativi all'utente e vengono utilizzati al fine di inviargli messaggi pubblicitari in linea con le preferenze manifestate dallo stesso nell'ambito della navigazione. Nei casi di cookie di profilazione prima parte occorre sempre inserire il banner e richiedere il consenso ai visitatori.

Nelle "FAQ" del 31.12.2014 il Garante scrive che "per i cookie di terze parti installati tramite il sito, gli obblighi di informativa e consenso gravano sulle terze parti, ma il titolare del sito, quale intermediario tecnico tra queste e gli utenti, è tenuto a inserire nell'informativa estesa i link aggiornati alle informative e ai moduli di consenso delle terze parti stesse".

Nella "Scheda informativa del 5.6.2015" si chiarisce poi che "se sul sito i banner pubblicitari o i collegamenti con i social network sono semplici link a siti terze parti che non installano cookie di profilazione non c'è bisogno di informativa e consenso".

- *Notificazione*

  L'uso dei cookie rientra tra i trattamenti soggetti all'obbligo di notificazione (art. 37, c. 1, lett. d, Codice privacy) se finalizzati a "definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti".

  L'uso dei cookie è sottratto all'obbligo di notificazione (Provvedimento del Garante del 31.3.2004) se i trattamenti sono «relativi all'utilizzo di marcatori elettronici o di dispositivi analoghi installati, oppure memorizzati temporaneamente, e non persistenti, presso l'apparecchiatura terminale di un utente, consistenti nella sola trasmissione di identificativi di sessione in conformità alla disciplina applicabile, all'esclusivo fine di agevolare l'accesso ai contenuti di un sito Internet».

  Per il Garante, come da infografica del 10.6.2015, l'obbligo di notificazione si ha nel caso siano stati installati:

  - cookie profilazione prima parte;
  - cookie analitici terze parti se non sono stati adottati strumenti che riducono il potere identificativo dei cookie e se la parte terza non si è impegnata a non incrociare le informazioni contenute nei cookies con altre di cui già dispone.

  La notificazione deve essere effettuata compilando le schede presenti nella procedura on line, in particolare la tabella 6, accessibile dall'home page del sito istituzionale dell'Authority cliccando la sezione SERVIZI ONLINE.

- *Traccia del consenso*

  Il Gestore del sito ha l'obbligo di tenere traccia del consenso dell'utente; può utilizzare un cookie tecnico, così da non riproporre l'informativa breve a successiva visita dell'utente.

  L'utente, comunque, può sempre modificare la sua scelta sui cookie attraverso l'informativa estesa, che deve essere linkabile da ogni pagina del sito.

- *Sanzioni*

  – Omessa o inidonea informativa = da 6.000 a 36.000 Euro.

- Assenza del consenso = da 10.000 a 120.000 Euro.
- Omessa o incompleta notificazione = da 20.000 a 120.000 Euro.