cizio delle relative procedure informatiche, nei *database* e nei sistemi di elaborazione utilizzati per i trattamenti, nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza *(backup e disaster recovery)* effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente, documentando tali operazioni al più tardi entro trenta giorni successivi alla scadenza dei termini di cui all'art. 132 del Codice.

7.6. *Altre misure*
Audit log
Devono essere adottate soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi *database* utilizzati.

Tali soluzioni comprendono la registrazione, in un apposito *audit log*, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici.

I sistemi di *audit log* devono garantire la completezza, l'immodificabilità e l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad *auditing*. A tali scopi devono essere adottati, per la registrazione dei dati di *auditing*, anche in forma centralizzata per ogni impianto di elaborazione o per *datacenter*, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche.

Le misure di cui al presente paragrafo sono adottate nel rispetto dei princìpi in materia di controllo dei lavoratori sull'uso di strumenti elettronici, con particolare riguardo all'informativa agli interessati (*cfr. Provv.* 1° marzo 2007 [doc. *web* n. 1387522]).

7.7. *Audit interno–Rapporti periodici*
La gestione dei dati di traffico per finalità di accertamento e repressione di reati deve essere oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte dei titolari del trattamento, in modo che sia verificata costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati.

L'attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quelli cui è affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati.

I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di *Alerting* e di *Anomaly Detection*, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sull'effettiva cancellazione dei dati decorsi i periodi di conservazione.

L'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate.

L'esito dell'attività di controllo deve essere:
- comunicato alle persone e agli organi legittimati ad adottare decisioni e a esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della società;
- richiamato nell'ambito del documento programmatico sulla sicurezza nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza;
- messo, a richiesta, a disposizione del Garante o dell'autorità giudiziaria.

7.8. *Documentazione dei sistemi informativi*

I sistemi informativi utilizzati per il trattamento dei dati di traffico devono essere documentati in modo idoneo secondo i princìpi dell'ingegneria del *software*, evitando soluzioni documentali non corrispondenti a metodi descrittivi standard o di ampia accettazione.

La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di *input/output* dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema.

La documentazione va corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati.

La documentazione tecnica deve essere aggiornata e messa a disposizione dell'Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico.

7.9. *Cifratura e protezione dei dati*

I dati di traffico trattati per esclusive finalità di giustizia vanno protetti con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema. In particolare, devono essere adottate soluzioni che rendano le informazioni, residenti nelle basi di dati a servizio delle applicazioni informatiche utilizzate per i trattamenti, non intelligibili a chi non disponga di diritti di accesso e profili di autorizzazione idonei, ricorrendo a forme di cifratura od offuscamento di porzioni dei database o degli indici o ad altri accorgimenti tecnici basati su tecnologie crittografiche.

Tale misura deve essere efficace per ridurre al minimo il rischio che incaricati di mansioni tecniche accessorie ai trattamenti (amministratori di sistema, *database administrator* e manutentori *hardware* e *software*) possano accedere indebitamente alle informazioni registrate, anche fortuitamente, acquisendone conoscenza nel corso di operazioni di accesso ai sistemi o di manutenzione di altro genere, oppure che possano intenzionalmente o fortuitamente alterare le informazioni registrate.

Eventuali flussi di trasmissione dei dati di traffico tra sistemi informatici del fornitore devono aver luogo tramite protocolli di comunicazione sicuri, basati su tecniche crittografiche, o comunque evitando il ricorso alla trasmissione in chiaro dei dati. Protocolli di comunicazione sicuri devono essere adottati anche per garantire, più in generale, la sicurezza dei sistemi, evitando di esporli a vulnerabilità e a rischio di intrusione (a titolo esemplificativo, l'accesso interattivo in modalità "emulazione di terminale", anche per scopi tecnici, non deve essere consentito su canali non sicuri, così come deve essere evitata l'attivazione di servizi di rete non necessari che si possono prestare alla realizzazione di forme di intrusione).

7.10. *Tempi di adozione delle misure e degli accorgimenti*

Valutato il complesso delle misure e degli accorgimenti, tenuto conto del quadro delle cautele che emergono dalle risultanze ispettive essere già in atto presso i fornitori, nonché dei tempi tecnici necessari per completarne l'attuazione, anche alla luce di quanto emerso dalla consultazione pubblica, risulta dagli atti congruo fissare un termine transitorio per i trattamenti di dati in essere, prevedendo che tutti gli adempimenti di cui al presente punto 7 siano completati al più presto ed entro, e non oltre, il termine che è parimenti congruo stabilire per tutti i fornitori al 31 ottobre 2008. Entro tale termine, i fornitori dovranno dare conferma al Garante attestando formalmente l'integrale adempimento al presente provvedimento.

8. Applicazione di alcune misure a dati trattati per altre finalità

Le considerazioni svolte sulla natura particolarmente delicata dei dati di traffico, sulla necessità di garantire una tutela maggiormente efficace dei diritti e delle libertà delle persone e di prescrivere una più incisiva messa in sicurezza di dati rilevano anche per ogni altro trattamento di dati di traffico telefonico e telematico effettuato dai fornitori di cui al paragrafo 3.

Ciò, comporta l'improrogabile esigenza di assicurare che almeno alcuni tra gli accorgimenti e le misure di cui al precedente punto 7, limitatamente a quelli adattabili al caso di specie, siano applicati comunque dai predetti fornitori nell'ambito di analoghi trattamenti di dati di traffico telefonico e telematico effettuati per finalità non di giustizia, ma di fatturazione, pagamento in caso di interconnessione e commercializzazione di servizi, nel più breve periodo temporale indicato nel menzionato art. 123.

Per tali ragioni il Garante, contestualmente e distintamente da quanto va disposto ai sensi dell'art. 132, comma 5, del Codice, prescrive ai fornitori di cui al paragrafo 3, ai sensi dell'art. 17 del medesimo Codice, di adottare nel termine e con la modalità di cui al paragrafo 7.10. le misure e gli accorgimenti indicati nella lettera c) del seguente dispositivo.

Copia del presente provvedimento verrà trasmessa al Ministero della giustizia, anche ai fini della sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana a cura dell'Ufficio pubblicazione leggi e decreti, nonché, per opportuna conoscenza, all'Autorità per le garanzie nelle comunicazioni.

TUTTO CIÒ PREMESSO IL GARANTE

a) ai sensi degli artt. 17, 123 e 132, comma 5, del Codice, prescrive ai fornitori di servizi di comunicazione elettronica individuati nel paragrafo 3 di adottare nel trattamento dei dati di traffico telefonico e telematico di cui al paragrafo 4 le misure e gli accorgimenti a garanzia degli interessati individuate nel presente provvedimento, provvedendo a (*par.* 7):

1. adottare specifici sistemi di autenticazione informatica basati su tecniche di *strong authentication*, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, che si applichino agli accessi ai sistemi di elaborazione da parte di tutti gli incaricati di trattamento, nonché di tutti gli addetti tecnici (amministratori di sistema, di rete, di *database*) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore, qualunque sia la modalità, locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti. Per i dati di traffico trattati per esclusive finalità di accertamento e repressione dei reati, una di tali tecnologie deve essere basata sull'elaborazione di caratteristiche biometriche dell'incaricato, in modo tale da assicurare la presenza fisica di quest'ultimo presso la postazione di lavoro utilizzata per il trattamento. Tali modalità di autenticazione devono essere applicate anche a tutti gli addetti tecnici (amministratori di sistema, di rete, di *database*) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore. Relativamente ai soli addetti tecnici indicati al presente punto 1, qualora circostanze legate a indifferibili interventi per malfunzionamenti, guasti, installazioni *hardware* e *software*, aggiornamento e riconfigurazione dei sistemi, determinino la necessità di accesso informatico a sistemi di elaborazione che trattano dati di traffico in assenza di *strong authentication*, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B) al Codice, deve essere tenuta traccia dell'evento in un apposito "registro degli accessi", nonché delle motivazioni che li hanno determinati, con una successiva descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore.
2. adottare specifiche procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica

dei sistemi e delle basi di dati. Il fornitore deve definire e attribuire agli incaricati specifici profili di autorizzazione differenziando le funzioni di trattamento dei dati di traffico per finalità di ordinaria gestione da quelle per finalità di accertamento e repressione dei reati e distinguendo, tra queste ultime, gli incaricati abilitati al solo trattamento dei dati di cui al primo periodo di conservazione obbligatoria (art. 132, comma 1, del Codice) dagli incaricati abilitati anche al trattamento dei dati di cui al secondo periodo di conservazione obbligatoria (art. 132, comma 2, del Codice) e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato (art. 7 del Codice);

3. adottare, per la conservazione dei dati di traffico per esclusive finalità di accertamento e repressione di reati, sistemi informatici distinti fisicamente da quelli utilizzati per gestire dati di traffico anche per altre finalità, sia nelle componenti di elaborazione, sia di immagazzinamento dei dati (*storage*). I dati di traffico conservati per un periodo non superiore ai sei mesi dalla loro generazione possono, invece, essere trattati per le finalità di giustizia sia prevedendone il trattamento con i medesimi sistemi di elaborazione e di immagazzinamento utilizzati per la generalità dei trattamenti, sia provvedendo alla loro duplicazione, con conservazione separata rispetto ai dati di traffico trattati per le ordinarie finalità. Le attrezzature informatiche utilizzate per i trattamenti di dati di traffico per le esclusive finalità di giustizia di cui sopra devono essere collocate all'interno di aree ad accesso selezionato (ovvero riservato ai soli soggetti legittimati ad accedervi per l'espletamento di specifiche mansioni) e munite di dispositivi elettronici di controllo o di procedure di vigilanza che comportino la registrazione dei dati identificativi delle persone ammesse, con indicazione dei relativi riferimenti temporali. Nel caso di trattamenti di dati di traffico telefonico per esclusive finalità di giustizia, il controllo degli accessi deve comprendere una procedura di riconoscimento biometrico. Inoltre, nell'ambito dei trattamenti per finalità di accertamento e repressione di reati, una volta decorso il termine di cui al comma 1 dell'art. 132 del Codice, il fornitore deve trattare tali dati con modalità che consentano l'accesso differenziato su base temporale, tramite forme di separazione dei dati che garantiscano il rispetto del principio di finalità dei trattamenti e l'efficacia dei profili di autorizzazione definiti. Tale differenziazione può essere ottenuta mediante separazione fisica, predisponendo sistemi del tutto separati nelle componenti di elaborazione e di archiviazione, oppure mediante separazione logica, ovvero intervenendo sulla struttura delle basi di dati e/o sui sistemi di indicizzazione e/o sui metodi di accesso e/o sui profili di autorizzazione. Infine, il fornitore deve adottare misure idonee a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici in tempi compatibili con i diritti degli interessati e comunque non superiori a sette giorni;

4. designare specificamente gli incaricati che possono accedere ai dati di traffico conservati per le finalità di cui all'art. 132 del Codice, anche per consentire l'esercizio dei diritti di cui all'art. 7 del Codice medesimo. Il processo di designazione deve prevedere la documentata frequenza di una periodica attività formativa concernente l'illustrazione delle istruzioni, il rispetto delle misure di sicurezza e le relative responsabilità. Per quanto riguarda le richieste per l'esercizio dei diritti di cui all'art. 7 del Codice che comportano l'estrazione dei dati di traffico, nei limiti in cui ciò è consentito ai sensi dell'art. 8, comma 2, lettera *f*) del Codice, il fornitore deve conservare in forma specifica la documentazione comprovante l'idonea verifica dell'identità del richiedente ai sensi dell'art. 9 del Codice stesso, e adottare opportune cautele per comunicare i dati al solo soggetto legittimato in base al medesimo articolo;

5. rendere i dati di traffico immediatamente non disponibili per le elaborazioni dei sistemi informativi allo scadere dei termini previsti dalle disposizioni vigenti. Il fornitore deve cancellare o rendere anonimi senza ritardo tali

dati, in tempi tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei *database* e nei sistemi di elaborazione utilizzati per i trattamenti nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza *(backup e disaster recovery)* effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente e, al più tardi, documentando tale operazione entro i trenta giorni successivi alla scadenza dei termini di cui all'art. 132 del Codice;

6. adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi *database* utilizzati. Tali soluzioni comprendono la registrazione, in un apposito *audit log*, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici. I sistemi di *audit log* devono garantire la completezza, l'immodificabilità, l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad *auditing*. A tali scopi il fornitore deve adottare, per la registrazione dei dati di *auditing*, anche in forma centralizzata per ogni impianto di elaborazione o per *datacenter*, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche;
7. svolgere, con cadenza almeno annuale, un'attività di controllo interno per verificare costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati. Tale attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quelli cui è affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati. I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di *Alerting* e di *Anomaly Detection*, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sull'effettiva cancellazione dei dati decorsi i periodi di conservazione. L'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate. L'esito dell'attività di controllo deve essere: comunicato alle persone e agli organi legittimati ad adottare decisioni e ad esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della società; richiamato nell'ambito del documento programmatico sulla sicurezza nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza; messo, a richiesta, a disposizione del Garante o dell'autorità giudiziaria;
8. documentare i sistemi informativi utilizzati per il trattamento dei dati di traffico in modo idoneo secondo i princìpi dell'ingegneria del *software*, evitando soluzioni documentali non corrispondenti a metodi descrittivi *standard* o di ampia accettazione. La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di *input/output* dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema. La documentazione va corre-

data con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati. La documentazione tecnica deve essere aggiornata e messa a disposizione dell'Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico;

9. proteggere i dati di traffico trattati per esclusive finalità di giustizia con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema. Il fornitore deve adottare soluzioni che rendano le informazioni residenti nelle basi di dati a servizio delle applicazioni informatiche utilizzate per i trattamenti, non intelligibili a chi non disponga di diritti di accesso e profili di autorizzazione idonei, ricorrendo a forme di cifratura od offuscamento di porzioni dei *database* o degli indici o ad altri accorgimenti tecnici basati su tecnologie crittografiche. Tale misura deve essere efficace per ridurre al minimo il rischio che incaricati di mansioni tecniche accessorie ai trattamenti (amministratori di sistema, *database administrator* e manutentori *hardware* e *software*) possano accedere indebitamente alle informazioni registrate, anche fortuitamente, acquisendone conoscenza nel corso di operazioni di accesso ai sistemi o di manutenzione di altro genere, oppure che possano intenzionalmente o fortuitamente alterare le informazioni registrate. Eventuali flussi di trasmissione dei dati di traffico tra sistemi informatici del fornitore devono aver luogo tramite protocolli di comunicazione sicuri, basati su tecniche crittografiche, o comunque evitando il ricorso alla trasmissione in chiaro dei dati. Protocolli di comunicazione sicuri devono essere adottati anche per garantire più in generale la sicurezza dei sistemi evitando di esporli a vulnerabilità e a rischio di intrusione;

b) ai sensi dei medesimi artt. 17, 123 e 132, comma 5 del Codice, nonché dell'art. 157 del Codice, prescrive ai predetti fornitori titolari del trattamento di effettuare tutti gli adempimenti di cui alla precedente lett. a) al più presto e, comunque, entro e non oltre il termine del 31 ottobre 2008, dandone conferma al Garante attestando entro lo stesso termine l'integrale adempimento;

c) ai sensi dell'art. 17 del Codice prescrive ai medesimi fornitori titolari del trattamento di adottare, rispetto ai dati di traffico trattati per le finalità di cui all'art. 123 del Codice, entro e non oltre il termine del 31 ottobre 2008, dandone ai sensi dell'art. 157 del Codice conferma al Garante e attestando entro lo stesso termine l'integrale adempimento, i seguenti accorgimenti e misure (*par.* 8):

1. adottare specifici sistemi di autenticazione informatica basati su tecniche di *strong authentication*, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, che si applichino agli accessi ai sistemi di elaborazione da parte di tutti gli incaricati di trattamento nonché di tutti gli addetti tecnici (amministratori di sistema, di rete, di *database*) che abbiano la possibilità concreta di accedere ai dati di traffico custoditi nelle banche dati del fornitore, qualunque sia la modalità, locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti. Qualora circostanze eccezionali, legate a indifferibili interventi per malfunzionamenti, guasti, installazione *hardware* e *software*, aggiornamento e riconfigurazione dei sistemi, determinino la necessità di accesso a sistemi di elaborazione che trattano dati di traffico da parte di addetti tecnici in assenza di *strong authentication*, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B) al Codice in materia di protezione dei dati personali, deve essere tenuta traccia in un apposito "registro degli accessi" dell'eventuale accesso fisico ai locali in cui sono

installati i sistemi di elaborazione oggetto di intervento e dell'accesso logico ai sistemi, nonché delle motivazioni che li hanno determinati, con una descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore;

2. adottare procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati;
3. rendere i dati di traffico immediatamente non disponibili per le elaborazioni dei sistemi informativi allo scadere dei termini previsti dalle disposizioni vigenti, provvedendo alla loro cancellazione o trasformazione in forma anonima, in tempi tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei *database* e nei sistemi di elaborazione utilizzati per i trattamenti nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (*backup* e *disaster recovery*) effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente e, al più tardi, documentando tale operazione entro i trenta giorni successivi alla scadenza dei termini di conservazione (art. 123 del Codice);
4. adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi *database* utilizzati. Tali soluzioni comprendono la registrazione, in un apposito *audit log*, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici. I sistemi di *audit log* devono garantire la completezza, l'immodificabilità, l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad *auditing*. A tali scopi il fornitore deve adottare, per la registrazione dei dati di *auditing*, anche in forma centralizzata per ogni impianto di elaborazione o per *datacenter*, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche;
5. documentare i sistemi informativi utilizzati per il trattamento dei dati di traffico in modo idoneo secondo i princìpi dell'ingegneria del *software*, evitando soluzioni documentali non corrispondenti a metodi descrittivi *standard* o di ampia accettazione. La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di *input/output* dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema. La documentazione va corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati. La documentazione tecnica deve essere aggiornata e messa a disposizione dell'Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico;

d) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia anche ai fini della sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana a cura dell'Ufficio pubblicazione leggi e decreti, nonché, per opportuna conoscenza, all'Autorità per le garanzie nelle comunicazioni.

Roma, 17 gennaio 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

37 Adempimenti semplificati per il *customer care* (*) 15 novembre 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), con particolare riguardo agli artt. 2 e 13;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Francesco Pizzetti;

PREMESSO

1. Misure di semplificazione e trattamento di dati nell'ambito di servizi telefonici di assistenza e informazione al pubblico

1.1. La disciplina di protezione dei dati personali prevede che il trattamento dei dati deve assicurare un livello elevato di tutela dei diritti e delle libertà fondamentali *"nel rispetto dei princìpi di semplificazione, armonizzazione ed efficacia"* (art. 1, comma 2, del Codice).

Specifiche disposizioni attuano tali princìpi semplificando il contenuto e le modalità per informare gli interessati rispetto al trattamento, in particolare per quanto riguarda i servizi telefonici di assistenza e di informazione al pubblico (art. 13, commi 2 e 3, del Codice).

Il Garante intende sviluppare ulteriormente tali disposizioni attraverso il presente provvedimento che tiene conto del principio secondo cui l'informativa, quando i dati sono raccolti presso gli interessati, *"può non comprendere gli elementi già noti alla persona che fornisce i dati"* (art. 13, comma 2).

1.2. Numerosi soggetti pubblici e privati utilizzano in modo crescente servizi telefonici di assistenza e di informazione al pubblico nello svolgimento della propria attività istituzionale, professionale, commerciale o di natura personale.

Alcune scelte organizzative valorizzano il mezzo telefonico quale canale di contatto privilegiato con l'utenza, specie nell'ambito di società di grandi dimensioni e di enti pubblici, il che può accrescere l'economicità e l'efficienza nei servizi resi (*cfr.* in merito art. 3 dir. min. 21 dicembre 2001, Linee-guida in materia di digitalizzazione dell'amministrazione, in *G.U.* 5 febbraio 2002, n. 30; dir. min. 4 gennaio 2005, Linee-guida in materia di digitalizzazione dell'amministrazione, in *G.U.* 12 febbraio 2005, n. 35).

La gestione del flusso delle chiamate, attraverso appositi servizi di assistenza telefonica, può assumere in talune circostanze una particolare complessità, strutturandosi su un insieme integrato di sistemi informativi e di risorse umane.

A seconda delle caratteristiche dei servizi e dei relativi destinatari è possibile individuare una vasta gamma di funzioni. Tra le più ricorrenti, possono evidenziarsi quelle di informazione e/o di assistenza alla clientela (*cd. "customer care"*), con riferimento all'instaurazione e

(*) *G.U.* 7 dicembre 2007, n. 285
[doc. *web* n. 1462788]

all'esecuzione di rapporti contrattuali in vari contesti (prenotazione di servizi, *phone-banking*, ecc.), quelle svolte a vantaggio della collettività da parte di amministrazioni pubbliche (si pensi alle chiamate di pubblica utilità, incluse le chiamate ai numeri di emergenza) o soggetti privati anche per quanto riguarda servizi a sovrapprezzo di tipo sociale-informativo, di assistenza, di consulenza tecnico-professionale e di intrattenimento.

1.3. Il presente provvedimento riguarda solo le attività che comportano un trattamento di dati personali prestate in modalità *inbound*, ossia oggetto di una chiamata dell'interessato anche se effettuate senza la mediazione di un operatore (attraverso canali di comunicazione interamente automatizzati).

Non formano invece oggetto di esame i servizi *cd.* outbound, di solito ricorrenti nello svolgimento di attività di *tele-marketing*, nell'ambito delle quali vengono contattati destinatari di comunicazioni commerciali anche attraverso *call center*: al riguardo, vige infatti un apposito quadro normativo (*cfr.* art. 58 del Codice del consumo di cui al d.lg. 6 settembre 2005, n. 206; art. 130 del Codice in materia di protezione dei dati personali; in merito, *v.* pure i *Provv.* 30 maggio 2007 [doc. *web* n. 1412626, doc. *web* n. 1412610, doc. *web* n. 1412598, doc. *web* n. 1412557, doc. *web* n. 1412586].

1.4. Il Garante, tenendo anche conto delle indicazioni e delle richieste di chiarimento formulate (con specifico riguardo ai rapporti con i committenti) da un'associazione di categoria rappresentativa delle società di *call center* operanti in *outsourcing*, intende altresì precisare alcune modalità di comportamento da osservare nella gestione dei servizi telefonici di assistenza e informazione al pubblico (*v. infra* punti 2, 3, 4 e 5).

2. Tipologie di dati e modalità del loro trattamento

Nello svolgimento delle attività qui considerate possono essere utilizzate legittimamente solo le informazioni personali pertinenti e non eccedenti in relazione ai servizi richiesti, informazioni che sono di regola comunicate direttamente dall'interessato.

Le tipologie di informazioni trattate sono piuttosto varie comprendendo dati sia comuni (ad esempio, anagrafici o di natura economica), sia sensibili (si pensi, esemplificativamente, alle informazioni raccolte nell'ambito di servizi prestati da strutture sanitarie). Alcune informazioni personali sono trattate mediante sistemi automatizzati (ad esempio, con l'ausilio di risponditori vocali automatici o grazie a sistemi informatici integrati idonei a fornire informazioni sulla linea chiamante, attraverso il dispositivo di individuazione della medesima).

La raccolta anche automatizzata di tali informazioni da parte dell'operatore che gestisce il servizio di assistenza telefonica al pubblico può avvenire senza che gli interessati ne siano specificamente consapevoli, come ad esempio nel caso di registrazione automatica dei numeri chiamanti da terminali che lo consentono e che permettono, quindi, di risalire all'identità dei relativi utilizzatori.

In relazione a questo contesto il Garante, prima di provvedere in merito all'informativa agli interessati, intende richiamare l'attenzione degli operatori del settore su alcuni profili connessi a tale problematica, utili per assicurare una piena conformità del trattamento alle disposizioni vigenti in materia di protezione dei dati personali dei trattamenti effettuati nell'ambito dei servizi telefonici di assistenza e informazione al pubblico.

3. Titolare e responsabile del trattamento

3.1. Il soggetto pubblico e privato "titolare del trattamento" può svolgere le attività volte a fornire servizi di assistenza e di informazione al pubblico per via telefonica, tramite personale operante sotto la sua diretta autorità in qualità di "incaricato del trattamento" (art. 30 del Codice) o terzi cui è affidato il servizio all'esterno sulla base di contratti di collaborazione (*cd. outsourcing*) che disciplinano le modalità per prestare questa attività strumentale.

Questa seconda soluzione è volta ad assecondare legittime esigenze organizzative. Mentre in altre discipline settoriali possono essere previste specifiche cautele (si pensi, esemplificativamente, a quelle contenute nel Comunicato della Banca d'Italia, in *G.U.* 21 agosto 2002, n. 195, Esternalizzazione di attività di sportello e, sulla medesima materia, nella Comunicazione della Commissione nazionale per la società e la borsa n. Din/2073042 del 7 novembre 2002) la disciplina di protezione dei dati personali ammette e non ostacola tale esternalizzazione. L'outsourcer va però designato quale "responsabile del trattamento" preposto ad attuare in concreto le decisioni del "titolare del trattamento" sulle finalità e modalità del trattamento, sugli strumenti utilizzati e sulla sicurezza (artt. 4, 28 e 29 del Codice; *v.* pure *Provv.* 16 febbraio 2006, punto 6, [doc. *web* n. 1242592]).

3.2. Al fine di garantire una rigorosa osservanza dei princìpi di protezione dei dati personali (e apprestare una tutela più intensa a favore degli interessati), il Codice richiede che chi operi in tale veste debba essere particolarmente qualificato –dovendo essere *"individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza"* (art. 29, comma 2, del Codice)– e, nell'ambito dei compiti che gli sono assegnati, debba conformare il proprio operato alle istruzioni del *"titolare del trattamento"* (art. 29, commi 4 e 5, del Codice).

Il titolare del trattamento è chiamato a svolgere un'analisi anche preventiva al trattamento delle implicazioni che le modalità operative prescelte possono comportare in ordine ai diritti degli interessati, e a porre particolare cura nella valutazione delle capacità professionali, nonché dell'adeguatezza organizzativa del responsabile del trattamento, tenuto conto della natura dei dati trattati. Questa valutazione d'insieme deve riguardare anche l'adeguatezza delle soluzioni tecnico-organizzative e di quelle concernenti la sicurezza dei dati e dei sistemi.

In questo quadro assume una particolare criticità la situazione nella quale un medesimo outsourcer si trovi a gestire contemporaneamente, specie se in un contesto logistico di promiscuità, una pluralità di servizi di assistenza telefonica al pubblico per distinti committenti titolari del trattamento. Tale concorrenza di attività non deve tradursi, in concreto, in un abbassamento o in una banalizzazione dei livelli di sicurezza, né, tantomeno, in una sostanziale commistione tra i differenti insiemi di dati da utilizzare per prestare distinti servizi per più titolari.

Occorre poi assicurare le condizioni per uno svolgimento corretto e trasparente delle relazioni con l'utenza, la quale deve poter individuare in maniera univoca il titolare del trattamento con il quale viene in contatto tramite il servizio di assistenza telefonica al pubblico.

Acquista quindi rilievo l'opportunità di un'approfondita verifica che le parti e, in particolare, il "titolare del trattamento", dovrebbero effettuare in sede di stipula e di attuazione del contratto di fornitura del servizio.

Il titolare del trattamento deve esercitare in concreto reali funzioni di controllo della corretta attuazione delle decisioni che è chiamato ad assumere, anche per ciò che riguarda le modalità di consultazione ed eventuale riproduzione degli archivi del titolare posti a disposizione dell'*outsourcer* e in relazione alla cessazione del loro utilizzo all'atto dell'estinzione del rapporto contrattuale.

4. Finalità, necessità, pertinenza e non eccedenza dei dati trattati

4.1. Nel rendere il servizio di assistenza e di informazione al pubblico non devono essere utilizzati dati personali di abbonati e di utenti che non siano necessari per prestare il servizio, come può avvenire in caso di servizi di natura meramente informativa. Efficaci analisi e monitoraggi della funzionalità e dell'effettiva prestazione del servizio possono essere a volte compiuti a volte disponendo solo di dati statistici anonimi (art. 3 del Codice).

Il trattamento di dati personali che sia realmente necessario per il servizio (anche quando si tratta di dati non direttamente identificativi, ma agevolmente riconducibili a un soggetto identificabile come nel caso degli identificativi delle linee chiamanti) deve comunque avvenire nel rispetto dei princìpi di pertinenza e non eccedenza (artt. 3 e 11 del Codice).

4.2. Occorre assicurare un quadro di correttezza nei riguardi dell'utenza. In particolare, le informazioni raccolte devono essere utilizzate solo per scopi determinati, espliciti e legittimi. I soggetti privati devono di regola raccogliere il consenso informato qualora intendano utilizzare i dati per finalità diverse e compatibili, come nel caso del *marketing* o della creazione di profili relativi all'utenza (artt. 23 e 24 del Codice), mentre i soggetti pubblici devono operare pur sempre per dichiarate finalità istituzionali, nell'osservanza delle pertinenti disposizioni del Codice (*cfr.* artt. 18 ss. del Codice).

Eventuali registrazioni legittime del contenuto delle comunicazioni, effettuate con l'operatore o per il tramite di dispositivi automatici, possono essere conservate solo per un periodo di tempo necessario al corretto assolvimento delle operazioni richieste dagli utenti o alle eventuali esigenze di fatturazione, nei casi di servizi a pagamento, salva l'osservanza di specifici obblighi di legge che ne legittimino l'ulteriore conservazione.

5. Informativa agli interessati e modalità semplificate (art. 13, commi 2 e 3, del Codice)

5.1. I servizi di assistenza telefonica al pubblico sono prestati, non di rado, senza trattare specificamente dati di carattere personale.

In secondo luogo, nei casi in cui, sulla base del principio di necessità, occorre utilizzare alcune informazioni di carattere personale, è di regola possibile fornire alla clientela un'idonea informativa *una tantum* sulle finalità e sulle caratteristiche essenziali del trattamento, già in occasione dell'instaurazione del rapporto contrattuale che spesso precede i contatti telefonici con il servizio (si pensi, ad esempio, ai servizi di assistenza tecnica *post*-vendita).

In tutti questi casi, non è quindi necessario fornire un'informativa in occasione del contatto telefonico con il servizio.

5.2. Tuttavia, può verificarsi il caso in cui il servizio non è preceduto da un contratto o da contatti in occasione dei quali vi sia stata già la possibilità di informare adeguatamente l'interessato.

Anche per questi casi, non è però necessario informare l'interessato rispetto agli elementi che gli siano già noti in base alle circostanze del caso.

A questo riguardo, se si pone attenzione alle specifiche caratteristiche dei servizi di assistenza e di informazione al pubblico, si può infatti constatare agevolmente che diversi elementi che dovrebbero far parte dell'informativa (art. 13 del Codice) sono già chiaramente evidenti, in particolare per quanto riguarda:

a) gli estremi identificativi del titolare del trattamento (art. 13, comma 1, lett. *f*));
b) le varie circostanze che emergono comunque, sotto altro profilo, nel corso della conversazione telefonica (ad esempio, le conseguenze di un eventuale rifiuto di rispondere e la natura obbligatoria o facoltativa del conferimento: art. 13, comma 1, lett. *b*) e *c*));
c) la finalità del servizio e l'ambito di utilizzazione dei dati (art. 13, comma 1, lett. *a*) e *d*)), in particolare quando non si perseguono altri scopi quali quelli di *marketing* o di profilazione per i quali dovrebbe essere peraltro acquisito il consenso.

5.3. Per ogni altro caso in cui risulti comunque opportuno o necessario indicare alcuni elementi dell'informativa in occasione di un contatto telefonico, deve tenersi conto della peculiarità di questo mezzo di comunicazione e della natura dei servizi resi i quali devono poter essere svolti con celerità e senza costi aggiuntivi.

Il principio di semplificazione richiamato nell'art. 2 del Codice esige che ogni eventuale altro elemento da indicare all'interessato e che non gli sia stato eventualmente già spiegato gli venga comunque rappresentato con formule sintetiche, chiare e di immediata comprensione, anche mediante brevi messaggi preregistrati nel corso di eventuali tempi di attesa del servizio.

Come premesso, il Garante intende sviluppare ulteriormente tali modalità semplificate autorizzando coloro che prestano i servizi in esame a indicare la modalità attraverso la quale l'interessato potrà consultare o ascoltare a richiesta un'informativa più specifica, ad esempio mediante un sito *web* o tramite operatore o messaggio registrato ascoltabile digitando una cifra sulla tastiera del telefono (art. 13, comma 3, del Codice).

I fornitori del servizio titolari del trattamento sono già autorizzati ad avvalersi di tutte le predette opportunità senza rivolgere al Garante alcuna richiesta, da formulare eventualmente solo per specifiche situazioni ritenute meritevoli di apposito esame.

5.4. Va infine disposto che i servizi abilitati in base alla legge a ricevere chiamate d'emergenza (d.m. Min. comunicazioni 27 aprile 2006 sul servizio "112" quale numero unico europeo d'emergenza; *v.* anche *Parere* del Garante 6 aprile 2006, [doc. *web* n. 1269346]), attesa la loro peculiare natura, possano rendere l'informativa agli interessati (se dovuta in base al Codice: *cfr.* art. 53) inserendola nei siti *web* di riferimento.

TUTTO CIÒ PREMESSO IL GARANTE

1. individua le seguenti linee-guida per i titolari del trattamento che prestano servizi di assistenza e di informazione al pubblico, in particolare ove si avvalgano di soggetti esterni designati "responsabili del trattamento" (punti 2, 3, 4 e 5):

   a. la raccolta delle informazioni personali deve limitarsi a quelle pertinenti e non eccedenti in relazione ai servizi richiesti;
   b. deve essere effettuata una previa analisi delle implicazioni che il trattamento di dati personali mediante servizi di assistenza telefonica al pubblico potranno comportare, anche tenuto conto della natura dei dati trattati;
   c. il contratto di fornitura del servizio di assistenza telefonica al pubblico deve contenere concrete modalità operative idonee ad assicurare condizioni di trasparente e corretto svolgimento delle relazioni con l'utenza, indicando altresì le misure di sicurezza idonee che dovranno essere adottate, anche al fine di prevenire commistioni tra distinti archivi gestiti dal medesimo responsabile del trattamento;
   d. deve essere posta particolare cura, ai sensi dell'art. 29 del Codice, nella valutazione delle capacità professionali e dell'adeguatezza organizzativa della struttura deputata a svolgere la funzione di servizi di assistenza telefonica al pubblico;
   e. le informazioni raccolte devono essere utilizzate solo per scopi determinati, espliciti e legittimi;
   f. eventuali registrazioni legittime del contenuto delle comunicazioni possono essere conservate solo per un periodo di tempo necessario al corretto assolvimento delle operazioni richieste dagli utenti o alle eventuali esigenze di fatturazione;
   g. non è necessario fornire l'informativa quando non sono trattati dati personali o in relazione ai diversi elementi già noti all'interessato; nei soli casi in cui è invece necessario rappresentare alcuni elementi, vanno comunque utilizzate formule sintetiche, chiare e di immediata comprensione;

2. autorizza i titolari del trattamento che prestano servizi di assistenza e di informazione al pubblico anche con la collaborazione di terzi designati responsabili del trattamento, ai sensi dell'art. 13, comma 3, del Codice, a rappresentare in modo semplificato ad abbonati e utenti interessati gli eventuali elementi dell'informativa che risulti necessario fornire, indicando la modalità attraverso la quale l'interessato potrà consultare o ascoltare a richiesta un'informativa più specifica, ad esempio mediante un sito *web* o tramite operatore o messaggio ascoltabile digitando una cifra sulla tastiera del telefono (punto 5.3.);

3. autorizza i servizi abilitati in base alla legge a ricevere chiamate d'emergenza, ai sensi dell'art. 13, comma 3, del Codice, a rendere l'informativa semplificata inserendola in un sito Internet (punto 5.4.);

4. dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 15 novembre 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

38 Bollette telefoniche: indicazione delle ultime tre cifre (*)

13 marzo 2008

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice");

Visto il provvedimento adottato dal Garante il 5 ottobre 1998 (in *www.garanteprivacy.it* doc. *web* n. 40751) sulla non menzione, nella fatturazione dettagliata, da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico, delle ultime tre cifre dei numeri telefonici chiamati; visto altresì il parere reso in materia da questa Autorità al Ministero delle comunicazioni il 5 ottobre 1999 (in *www.garanteprivacy.it* doc. *web* n. 39881);

Visto l'art. 124, comma 4, del Codice il quale stabilisce che nella fatturazione all'abbonato non sono evidenziate le ultime tre cifre dei numeri chiamati;

Visto l'art. 124, comma 2, del Codice che prevede l'obbligo per il fornitore del servizio di comunicazione elettronica accessibile al pubblico di abilitare l'utente a effettuare comunicazioni e a richiedere servizi da qualsiasi terminale, gratuitamente e in modo agevole, avvalendosi per il pagamento di modalità alternative alla fatturazione, anche impersonali, quali carte di credito o di debito o carte prepagate;

Rilevato che l'art. 124, comma 5, del Codice prevede che il Garante, accertata l'effettiva disponibilità delle predette modalità alternative alla fatturazione indicate al comma 2 del medesimo articolo, può autorizzare il fornitore a indicare nella fatturazione dettagliata richiesta dagli abbonati i numeri completi delle comunicazioni;

Vista l'istruttoria preliminare avviata dall'Autorità nel corso dell'anno 2007 volta a verificare il rispetto della disciplina in materia di protezione dei dati personali, relativamente all'effettiva e diffusa disponibilità per abbonati e utenti di modalità di pagamento alternative alla fatturazione, anche impersonali, ai sensi dell'art. 124, comma 2, del Codice;

VISTI gli elementi acquisiti, nei quali i principali fornitori di servizi di comunicazione elettronica accessibili al pubblico hanno attestato, sotto la propria responsabilità, di aver abilitato i propri utenti a effettuare comunicazioni e a richiedere servizi mediante l'utilizzo di modalità alternative alla fatturazione;

Rilevato che la maggior parte dei predetti fornitori ha altresì attestato, sotto la propria responsabilità, di aver attualmente reso reperibili sul territorio nazionale proprie modalità alternative alla fatturazione, anche di tipo impersonale, quali carte a codice e carte prepagate, oppure di aver abilitato i propri utenti all'uso di carte di debito o di credito;

Tenuto conto che i fornitori hanno altresì attestato che tali carte sono fruibili e distribuite sul territorio, essendo acquistabili presso tabaccherie, edicole, siti *web*, circuiti bancari Atm e ricevitorie della rete Sisal o Lottomatica, nonché presso negozi dove sono disponibili prodotti dei fornitori;

Considerato che, nell'ambito dell'istruttoria preliminare compiuta è emerso che, oltre a

(*) *G.U.* 3 aprile 2008, n. 79
[doc. *web* n. 1501106]

modalità alternative alla fatturazione messe a disposizione direttamente da fornitori, ve ne sono altre che risultano distribuite da parte di soggetti diversi dai fornitori di servizi di comunicazione elettronica (*ad es.*, Poste italiane S.p.A.);

Tenuto conto che dagli elementi acquisiti nell'ambito dell'istruttoria preliminare emerge anche che, rispetto al periodo in cui è stato disciplinato il mascheramento delle ultime tre cifre, si è registrato un enorme incremento dell'utilizzo della telefonia mobile con particolare riferimento a quella *cd.* prepagata, che costituisce di per sé una sostanziale modalità alternativa di pagamento (allo stato, le linee attive risultano superare gli 80 milioni e, di queste, l'89% risulta appartenere alla categoria delle prepagate);

Viste le osservazioni del 6 febbraio 2008 formulate da parte dell'associazione di categoria rappresentativa dei maggiori fornitori di servizi di telecomunicazioni, (Assotelecomunicazioni-Asstel);

Considerato che sussistono, allo stato, le condizioni per adottare un provvedimento generale di carattere autorizzativo ai sensi dell'art. 124, comma 5, del Codice rivolto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che abbiano abilitato i propri utenti a effettuare comunicazioni e a richiedere servizi mediante l'utilizzo delle predette modalità alternative;

Tenuto conto che i dati contenuti nelle fatture dettagliate attengono ad aspetti della vita privata che riguardano il chiamante, l'abbonato e il chiamato; rilevato che è necessario contemperare i rispettivi diritti e che si rende, quindi, necessario adottare il presente provvedimento di carattere autorizzativo ai sensi dell'art. 124, comma 5, del Codice;

Ritenuto che i fornitori di servizi di comunicazione elettronica accessibili al pubblico che intendano avvalersi della facoltà prevista per legge e dal presente provvedimento dovranno informare preventivamente della decisione di esercitare tale facoltà tutti i rispettivi abbonati mediante un'idonea informativa da inserire all'interno di almeno due fatture e nel proprio sito *web*;

Considerato che la società che si avvale della presente autorizzazione è tenuta, in ogni caso, a offrire ai propri abbonati che lo richiedano la possibilità di ricevere la fatturazione con le ultime tre cifre *"mascherate"*;

Considerato che l'informativa dei fornitori dovrà specificare agli abbonati che abbiano richiesto o intendano richiedere la fatturazione dettagliata che la riceveranno *"in chiaro"*; che in tale informativa il fornitore dovrà inserire un invito agli abbonati a informare coloro che utilizzano l'utenza che la fatturazione perverrà completa dei numeri chiamati relativi alle comunicazioni documentate nella fatturazione dettagliata; che dovrà essere altresì indicato agli abbonati, che su loro specifica richiesta, essi potranno ricevere la fatturazione con le ultime tre cifre *"mascherate"*;

Ritenuto che, in ragione della richiesta di Assotelecomunicazioni-Asstel di stabilire una data unica per gli operatori, appare congruo indicare nel 1° luglio 2008 la data a partire dalla quale tutti i fornitori di comunicazione elettronica accessibili al pubblico, sempreché essi abbiano abilitato i propri utenti a effettuare chiamate e a richiedere servizi nei termini sopra indicati, potranno indicare i numeri completi delle comunicazioni nella fatturazione dettagliata;

Visto che copia del presente provvedimento verrà trasmessa al Ministero della giustizia, anche ai fini della sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana a cura dell'Ufficio pubblicazione leggi e decreti, nonché, per opportuna conoscenza, all'Autorità per le garanzie nelle comunicazioni.

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 del 28 giugno 2000;

Relatore il prof. Francesco Pizzetti;