Athena

LE RECENTI MODIFICHE AL CODICE DELLA PRIVACY INTRODOTTE DAL D.LGS 69/2012

Il Governo con D.Lgs. 28 maggio 2012 n. 69 ha dato attuazione alla delega prevista nella Legge comunitaria del 2010 (L. 217/2011) per il recepimento delle direttive 2009/136/CE in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, 2009/140/CE in materia di reti e servizi di comunicazione elettronica e del regolamento n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori.

Il citato decreto apporta significative modifiche al d.lgs. 196/2003 (Codice Privacy), in merito alla disciplina applicabile ai **fornitori di servizi di comunicazione elettronica accessibile al pubblico**, mettendo in luce la costante sensibilità del legislatore, comunitario e nazionale, nei confronti della tutela dei dati personali nell'ambito della comunicazione elettronica.

Già nella legge delega, che ha portato all'emanazione del decreto legislativo, viene stabilito che, nel settore del trattamento dei dati personali deve essere assicurato il rispetto dei principi e dei criteri direttivi specifici destinati al rafforzamento delle prescrizioni in tema di sicurezza e riservatezza delle comunicazioni, nonché di protezione dei dati personali e delle informazioni già archiviate nell'apparecchiatura terminale, fornendo all'utente indicazioni chiare e comprensibili circa le modalità di espressione del proprio consenso, in particolare mediante le opzioni dei programmi per la navigazione nella rete Internet o altre applicazioni.

Tra le modifiche introdotte da tale decreto al Codice Privacy, è innanzitutto da considerare il **nuovo concetto di "violazione di dati personali"** (art. 4,co.3, lett. g bis) definita come la *"violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico"*.

Sulla base di questa definizione sono da considerare le modifiche apportate al titolo V rubricato "Sicurezza dei dati e dei sistemi" che hanno ristrutturato l'**art. 32** e introdotto l'**art. 32 bis**, i quali prevedono, rispettivamente, le misure di sicurezza che i fornitori di servizi di comunicazione elettronica accessibili al pubblico debbono adottare per prevenire le anzidette violazioni e gli adempimenti da porre in essere in seguito al verificarsi di una violazione di dati personali.

L'articolo 32 del Codice Privacy, in particolare, che già prevedeva l'adozione da parte dei fornitori di misure tecniche e organizzative adeguate per salvaguardare la sicurezza dei servizi di comunicazione elettronica accessibile al pubblico, in seguito all'entrata in vigore del d.lgs. 68/2012 prevede altresì l'adozione di misure relative agli adempimenti di cui al successivo articolo 32 bis.

Alla luce di tale modifica, inoltre, **il fornitore può, ora, adottare le misure di sicurezza anche attraverso altri soggetti a cui sia affidata l'erogazione del servizio** di comunicazione elettronica accessibile al pubblico.

Inoltre, ai sensi dell'art. 32, i fornitori devono garantire che l'**accessibilità dei dati** sia permessa **solo al personale autorizzato per fini legalmente autorizzati** e devono garantire la protezione dei dati relativi al traffico, all'ubicazione e degli altri dati personali archiviati o trasmessi, dalla distruzione anche accidentale, dalla perdita o alterazione anche accidentale e dalla archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti assicurando, inoltre, l'attuazione di una politica di sicurezza.

Ed ancora, se in precedenza era previsto che, nel caso di sussistenza di un particolare rischio di violazione della sicurezza della rete il fornitore di un servizio di comunicazione elettronica accessibile al pubblico avesse

l'obbligo di informare il Garante, gli abbonati e, ove possibile, gli utenti, ora con l'introduzione dell'articolo 32 bis, che individua gli **"Adempimenti conseguenti ad una violazione di dati personali"**, il legislatore pone tutta una serie di obblighi di comunicazione in capo al fornitore tali da mettere in moto un meccanismo in cui tutte le parti interessate (fornitore, contraente, utente e Garante Privacy) cooperino al fine di limitare eventuali danni.

Ai sensi del nuovo art. 32 bis, in caso di violazione di dati personali nei servizi di comunicazione elettronica accessibili al pubblico, il fornitore:

- **comunicherà**, senza ritardo, **all'Autorità Garante Privacy** le violazioni dei dati personali;
- se la violazione rischia di arrecare pregiudizio anche ai dati personali o alla riservatezza del contraente o di altra persona, il fornitore comunicherà anche agli stessi e senza ritardo l'avvenuta violazione. È previsto che tale comunicazione potrà essere omessa nel solo caso in cui il fornitore dimostri al Garante di aver utilizzato misure tecnologiche di protezione che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate ai dati oggetto della violazione.

Se in seguito a eventuali violazioni sono presumibili ripercussioni negative, e il fornitore non vi abbia già provveduto, il Garante potrà comunque intervenire obbligando il fornitore a **comunicare l'avvenuta violazione al contraente o ad altra persona**.

Il legislatore ha previsto anche il contenuto minimo che le suddette comunicazioni agli interessati dovranno contenere:

1. descrizione della natura della violazione di dati personali;
2. punti di contatto presso cui si possano ottenere maggiori informazioni;
3. elenco delle misure che il fornitore consiglia di adottare per attenuare i possibili effetti pregiudizievoli della violazione.

La comunicazione al Garante dovrà contenere, inoltre, la descrizione delle conseguenze della violazione di dati personali e le misure proposte o adottate dal fornitore per porvi rimedio.

E' stata inoltre prevista dal comma 6 dell'articolo 32 bis del Codice, la possibilità per il Garante di emanare un provvedimento o delle linee guida con il quale illustrare orientamenti e istruzioni in relazione alle circostanze in cui il fornitore ha l'obbligo di comunicare le violazioni di dati personali, il formato applicabile a tale comunicazione, nonché alle relative modalità di effettuazione, tenuto conto delle eventuali misure tecniche di attuazione adottate dalla Commissione europea.

Il decreto ha inoltre stabilito, per consentire al Garante di verificare il rispetto delle disposizioni di legge, che i fornitori dovranno tenere un aggiornato **inventario delle violazioni** di dati personali all'interno del quale indicheranno le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti adottati per porvi rimedio.

La violazione di tali obblighi è oggetto di severe sanzioni amministrative previste dall'art. 162ter e penali previste dal riformato art. 168. In particolare, è prevista una sanzione amministrativa dai 25.000 ai 150.000 euro per l'omessa comunicazione al Garante e dai 20.000 ai 120.000 euro per l'omissione dell'inventario delle violazioni; l'omessa comunicazione ai contraenti o alle altre persone interessate, seppure nei limiti del 5% del volume d'affari e con ulteriori limiti nei casi di minore gravità, comporta una sanzione da un minimo di 150 euro fino a un massimo di 1.000 euro per ogni singola comunicazione omessa.

La normativa prevede inoltre che, nel caso in cui il fornitore di un servizio di comunicazione elettronica accessibile al pubblico affidi l'erogazione del predetto servizio ad altri soggetti, gli stessi sono tenuti a comunicare al fornitore senza indebito ritardo tutti gli eventi e le informazioni necessarie a consentire a

quest'ultimo di effettuare gli adempimenti di cui al presente articolo. Dato ciò, le medesime sanzioni previste per i fornitori si applicheranno anche nei confronti dei soggetti a cui il fornitore di servizi di comunicazione elettronica accessibili al pubblico abbia affidato l'erogazione dei predetti servizi qualora tali soggetti non abbiano comunicato tempestivamente le informazioni necessarie in modo da permettere al fornitore di adempiere agli obblighi di legge.

Sono stati oggetto di importanti modifiche, inoltre, anche gli artt. 121, 122, 123, 130, 164 bis e 168 del Codice Privacy.

È stato innanzitutto **ampliato l'ambito di applicazione delle norme del titolo X sulle comunicazioni elettroniche** al trattamento dei dati personali connessi non solo alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche, ma anche a quelle che supportano i dispositivi di raccolta dei dati e di identificazione.

Molto opportunamente poi, la nuova formulazione dell'art. 122, limita e disciplina l'accesso dei fornitori di servizi di comunicazione elettronica alle informazioni raccolte nei riguardi dei propri abbonati od utenti, prevedendo che "L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con le modalità semplificate di cui all'articolo 13, comma 3. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio."

Al di fuori di questa casistica non è, in ogni caso, consentito l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente stesso (comma 2-bis).

Sulla problematica relativa all'**acquisizione del consenso**, invece, al secondo comma dell'art. 122 viene stabilito che "Ai fini dell'espressione del consenso di cui al comma 1, possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente", lasciando spazio così a una eventuale acquisizione informatica o telematica del consenso del contraente o dell'utente (persona fisica) interessati al trattamento.

Infine, è stata imposta ai fornitori l'adozione di procedure interne per corrispondere alle richieste effettuate in conformità alle disposizioni comunitarie che prevedono "forme di accesso a dati personali degli utenti", sotto la vigilanza del Garante. Infatti, la citata direttiva 2002/58/CE Art. 15, paragrafo 1-ter, prevede che i fornitori di servizi di telecomunicazione istituiscono procedure interne per rispondere alle richieste di accesso ai dati personali degli utenti e, su richiesta, forniscono alla competente autorità nazionale informazioni sulle procedure esperite. Orbene il nuovo art. 132 bis prevede che "I fornitori istituiscono procedure interne per corrispondere alle richieste effettuate in conformità alle disposizioni che prevedono forme di accesso a dati personali degli utenti." E con riferimento alle competenze del Garante si precisa che i fornitori su richiesta debbono fornire le informazioni sulle procedure interne, sul numero di richieste ricevute, sui motivi legali addotti e sulle risposte date.

Va in ultimo rilevato che, con un intervento trasversale, il comma 12 dell'art. 1 prevede che nel Codice, la parola: "abbonato", ovunque ricorra, sia sostituita dalla seguente: "contraente".

La definizione del termine "contraente" pone però alcuni problemi interpretativi; il Legislatore ha infatti

lasciato inalterata la definizione prima riferita all'abbonato: "qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate". Tale definizione mal si coordina con la fondamentale definizione di "dato personale" così come risulta modificata dal D.L. 6 dicembre 2011, n. 201, secondo cui può essere considerato tale "qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale". Il D.L. 201 ha eliminato, infatti, qualunque riferimento alle persone giuridiche, enti o associazioni che invece compaiono nella definizione di contraente. Tale mancato coordinamento, dovuto probabilmente ad un *lapsus* del Legislatore, conduce a esiti imprevisti.

Il termine "contraente", viene , in rilievo, innanzi tutto, nel quadro del nuovo articolo 32 bis; ai sensi del secondo comma, infatti, "quando la violazione di dati personali rischia di arrecare pregiudizio ai dati personali o alla riservatezza di contraente o di altra persona, il fornitore comunica anche agli stessi senza ritardo l'avvenuta violazione". Per "violazione di dati personali", il Codice intende una "violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico". Di conseguenza, una interpretazione non contraddittoria delle due definizioni deve portare a ritenere che il rischio di arrecare pregiudizio ai dati personali o alla riservatezza potrà concretizzarsi solo in relazione ai quei contraenti che siano persone fisiche poiché sono dati personali solo le informazioni che si riferiscono a questo tipo di soggetti; per lo stesso motivo gli obblighi di comunicazione dell'avvenuta violazione al contraente imposti dal Garante vanno riferiti ai soli contraenti persone fisiche.

Il "contraente", viene in rilievo anche in relazione alla previsione dell'art. 122, così come modificato proprio dal D.lgs. 69/12 che vieta, in termini generali, "l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente". In questo caso l'utilizzo del termine "informazioni" *in senso lato* (al posto di "dato personale") rende la previsione applicabile a tutti i contraenti anche quelli diversi dalle persone fisiche; In tutti i casi contemplati dall'art. 122 oggetto di protezione sono generiche informazioni e non solo dati personali e quindi coerentemente tra i soggetti legittimati a prestare il loro consenso o ad opporsi ad accessi illegittimi negli apparecchi terminali ci sono anche i contraenti persone giuridiche.