

SENZA LA PROROGA
Dati telefonici
da cancellare
A rischio anche
le indagini penali

Candidi e Monti ▶ pagina 31

Giustizia. Scaduto il 30 giugno l'obbligo di conservazione (anche degli accessi internet) oltre i termini del codice della privacy

Vecchi dati telefonici da distruggere

L'impatto sulle inchieste per terrorismo e mafia - Il ministero: dalle procure nessun allarme

IL CASO FRANCESE

Per esigenze investigative sulle cellule terroristiche l'Eliseo ha allungato i tempi di utilizzo delle comunicazioni
Andrea Maria Candidi

■ Scade l'obbligo, per gli operatori telefonici e gli internet provider, di conservare i dati del traffico telefonico e telematico più vecchi, precedenti cioè i termini ordinari di conservazione. Ed è allarme sulle inchieste per i reati più gravi, mafia o terrorismo, che di questi termini più ampi si sono fin qui potute giovare.

L'obbligo sulla cosiddetta data-retention è stato introdotto dal decreto antiterrorismo del 2015 (Dl n. 7) che per esigenze investigative ha imposto, fino al 30 giugno 2017, il mantenimento di tutti i dati di traffico, in deroga ai vincoli del codice della privacy, a partire dal 21 aprile 2015 (data di entrata in vigore della legge di conversione del decreto legge antiterrorismo).

Ora, superata la scadenza del 30 giugno senza che il legislatore sia intervenuto, tornano ad applicarsi le regole base, quelle cioè previste dal codice della privacy per cui i

dati del traffico telefonico devono essere conservati per 24 mesi dalla comunicazione e quelli telematici per 12 mesi. Ciò vuol dire che, oggi, i gestori telefonici devono tenere solo le informazioni relative alle comunicazioni effettuate da due anni a questa parte (cioè, dal 3 luglio 2015 fino a oggi), mentre gli operatori internet devono conservare i dati relativi agli accessi dell'ultimo anno (vale a dire dal 3 luglio 2016 a oggi). Di conseguenza, tutti i dati precedenti, possono (devono?) essere distrutti da chi li detiene.

Con buona pace delle inchieste sui reati più gravi, dal terrorismo alla mafia come detto, che il decreto legge del 2015 intendeva invece tutelare (si veda l'altro articolo in pagina). Sul punto, dal ministero della Giustizia smorzano qualsiasi allarmismo e fanno sapere che le regole e i termini sono quelli in vigore, dunque senza l'obbligo di conservazione generalizzato. A deroghe, ribadiscono da Via Arenula, ci si penserà eventualmente qualora dovessero giungere allarmi dalle procure, che però al momento - sottolineano - non sono stati registrati.

Quella dei dati chiesti sistematicamente dagli inquirenti e dagli organi di polizia giudi-

ziaria è «una messe imponente» spiega l'avvocato Fulvio Sarzana, legale rappresentante di Assoprovider: «Per poter conservare tutte queste informazioni - sottolinea - i fornitori dei servizi di comunicazione elettronica devono spendere cifre considerevoli». Va peraltro ricordato che molte comunicazioni solo apparentemente sono telefoniche, ma servizi voce come Voip generano di fatto traffico telematico.

Vedremo, in ogni caso, come si comporteranno le aziende del settore e se e come il legislatore intende risolvere la questione.

Vero è che, nonostante i vincoli europei (si ricorda che i giudici di Lussemburgo hanno bocciato la data-retention indiscriminata, cioè senza limiti) l'ondata di terrorismo di matrice islamica che sta investendo il Vecchio continente ha imposto agli stati membri di adottare misure emergenziali che derogano, senza andare troppo per il sottile, alle regole. La Francia, ad esempio, ha ampiamente superato i vincoli delle regole comunitarie con la nuova normativa antiterrorismo che impone la conservazione di tutti i dati di traffico telefonico e telematico.

© RIPRODUZIONE RISERVATA





LA PAROLA
CHIAVE

Data-retention

- La data-retention è la disciplina per la conservazione dei dati di traffico telefonico e telematico, i dati relativi all'ubicazione e necessari all'identificazione dell'abbonato, per fini di accertamento e repressione dei reati. La Corte Ue ha bocciato la direttiva 2006/24/Ce per violazione del principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza.