In base all'art.76 del D.P.R. 445 del 28 dicembre 2000 il rilascio di dichiarazioni mendaci, la formazione o l'uso di atti falsi sono puniti ai sensi del codice penale e dalle leggi speciali in materia. Gli operatori telefonici effettuano verifiche sulla titolarità delle utenze mobili, prevedendo la possibilità di compilare un modulo per segnalare l'eventuale disconoscimento della titolarità di un'utenza che non è mai stata richiesta o per la quale non si è mai sottoscritto alcun abbonamento.

Roberto COSA è Direttore *Business Security* di 3 Italia (H3G S.p.A.). Dal 1978 al 2001 è Ufficiale dei Carabinieri (Ten. Col. r.), con incarichi territoriali e di Stato Maggiore. Dal 2001 al 2004 è responsabile della sicurezza del Gruppo De Agostini e Amministratore unico di Società del Gruppo. Dal 2004 al 2005 è responsabile Sicurezza e analisi dei Rischi di Ferrovie dello Stato.

L'IDENTITÀ DEL PARLANTE

di Roberto COSA

Il mondo delle prestazioni obbligatorie, previsto normativamente dall'art. 96 del Codice delle Comunicazioni elettroniche, costituisce uno degli impegni di maggior importanza e delicatezza per gli operatori delle telecomunicazioni, per le evidenti conseguenze correlate all'utilizzo delle informazioni sottostanti alle prestazioni stesse, che spesso si trasformano in elementi di prova nell'ambito di procedimenti penali.

Responsabilità diretta dell'operatore, che non si deve limitare quindi alla mera trasmissione di dati, ma **deve "certificare"** la correttezza degli stessi, motivo per il quale l'attività interna non impatta le sole strutture dedicate alla gestione delle prestazioni obbligatorie, ma è costante una stretta sinergia con la Rete, specie per quanto riguarda le informazioni sul passaggio delle comunicazioni sulle celle.

In questo scenario, se le intercettazioni e il traffico storico sono garantiti nella loro completezza da sistemi e infrastrutture che rispondono a requisiti e standard *ad hoc*, non altrettanto si può dire delle anagrafiche per una serie strutturale di criticità ben note agli addetti ai lavori. Tra tutte, **la presenza di documenti falsificati difficilmente riconoscibili**, l'impossibilità di accedere alle banche dati dei documenti rubati o smarriti, l'elevato numero di frodi, che colpisce peraltro tutti i settori merceologici, e i reati che sono correlati all'utilizzo delle tecnologie di comunicazione sociale, primi tra tutti i furti di identità, per la facilità di reperimento delle informazioni anche da parte di "utenti" di media capacità. Dal punto di vista del *business*, per gli operatori la fattispecie ha un impatto economico notevole, andando ad incidere in maniera consistente sui costi legati al traffico non pagato e soprattutto alla perdita dei telefoni, tutti ormai ad alto valore, con l'impossibilità di identificare il frodatore e attivare rimedi di natura legale e/o giudiziaria.

Tra i rimedi messi in piedi, più o meno a fattor comune, le attività dei dipartimenti antifrode, i processi di formazione sulla tematica erogati alla rete vendita, le azioni di "*mistery shopping*" per verificare il rispetto delle regole imposte e la correttezza delle attivazioni da parte della rete di vendita, i corsi tenuti sulle caratteristiche dei documenti, con particolare riguardo ai permessi di soggiorno e le innumerevoli denunce presentate su tutto il territorio nazionale.

Il secondo aspetto di criticità è ovviamente quello di interesse per le prestazioni obbligatorie nella parte relativa all'identificazione dell'acquirente della SIM, che incide sulle capacità info-investigative delle Autorità richiedenti. In questo, la situazione diventa ancora più impegnativa soprattutto quando il contesto di riferimento si allarga all'Unione Europea, data la asimmetria in materia di legislazioni nazionali circa l'obbligatorietà di identificazione.

Attualmente in Italia la normativa deriva:

- dall'art. 55 del citato Codice delle Comunicazioni elettroniche modificato dalla legge 155/2005 (cd. Pisanu) che recita: "*ogni impresa è tenuta a rendere disponibili, anche per via telematica, al centro di elaborazione dati del Ministero dell'interno gli elenchi di tutti i propri abbonati e di tutti gli acquirenti del traffico prepagato della telefonia mobile, che sono identificati al momento dell'attivazione del servizio. L'Autorità giudiziaria ha facoltà di accedere per fini di giustizia ai predetti elenchi in possesso del centro di elaborazione dati del Ministero dell'interno*". Si tratta quindi di identificazione diretta, che prevede l'acquisizione da parte del venditore della copia del documento presentato dall'acquirente
- dal D.L.221 del 17 dicembre 2012,che all'art. 14 prevede: "*anche in deroga a quanto previsto dal comma 2, gli utenti che attivano schede elettroniche (S.I.M. – Subscriber Identity Module) abilitate al solo traffico telematico ovvero che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche o punti di accesso ad internet utilizzando tecnologia senza fili possono essere identificati e registrati anche in via indiretta, attraverso sistemi di riconoscimento via SMS e carte di pagamento nominative…*". In questo caso, l'identificazione è indiretta ed il dealer si avvale dell'identificazione effettuata in precedenza in ambito circuito bancario per il rilascio delle carte di credito.

La *ratio* della normativa è quindi quella di garantire l'identificabilità di chi acquista e utilizza le SIM, rendendo snelle le procedure nel caso di utente già identificato, anche in altro ambito.

Il discorso cambia radicalmente quando si entra nel contesto europeo. Infatti, a fronte dei 28 Paesi che compongono l'Unione Europea, **solo 12 richiedono l'identificazione dell'acquirente delle**

SIM, non necessariamente per fini di sicurezza o giustizia, mentre nei restanti 16 la vendita è sostanzialmente libera da obblighi di identificazione, fatte salve alcune eccezioni dove il cliente viene incentivato a lasciare i propri dati per motivi di marketing e di promozione. In Irlanda, a solo titolo esemplificativo, alcuni Operatori offrono traffico prepagato agli utenti che volontariamente acconsentono alla registrazione dei loro dati personali per motivi commerciali.

È evidente come la situazione delineata si presti a squilibri ed asimmetrie soprattutto quando si vanno ad impattare ambiti legati alle esigenze di pubblica sicurezza.
Il problema, tuttavia, non è legato solo alla mancanza di una direttiva Europea che vada ad uniformare il quadro normativo dei singoli Paesi - attualmente la Corte di Giustizia europea (Sentenza CGUE 08/04/2014 nelle cause riunite C-293/12 e C-594/12)[1] ha dichiarato invalida la direttiva 2006/24/EU che prevedeva l'identificazione degli acquirenti delle SIM a seguito degli attentati di Madrid e Londra – ma alla singola percezione degli Stati dove è stato introdotto l'obbligo di acquisire la documentazione di chi acquista le SIM.

La citata sentenza rappresenta una svolta nell'applicazione della normativa sulla c.d. *Data Retention* in quanto, con un importante cambio di indirizzo, si è passati dalla tutela dei dati si relativi al traffico, a quelli relativi all'ubicazione delle persone fisiche e giuridiche e ai dati connessi necessari per identificare l'abbonato o l'utente, ad un regime di invalidità di tali restrizioni e controlli in quanto lesivi del diritto al rispetto della vita privata e familiare, poiché si autorizzava una eccessiva (e dunque illegittima) ingerenza nel diritto alla protezione dei dati personali.
Inoltre, a titolo esemplificativo, si sottolinea che nel 2012 la Lituania ha chiesto alla Commissione europea di valutare l'opportunità di adottare una norma a livello europeo per rendere obbligatoria l'identificazione di chi compra SIM anche prepagate, a fronte del crescente numero di frodi telefoniche che ha colpito il Paese e dell'impossibilità per le Forze di Polizia di stabilire l'identità dei responsabili.

La Commissione ha quindi invitato gli Stati membri che hanno inserito misure del genere a fornire la prova dell'efficacia della registrazione obbligatoria delle SIM anche ai fini di Polizia, e la risposta è stata che non ci sono evidenze in termini di benefici per le indagini e di conseguenza vengono a mancare i presupposti per giustificare un'azione a livello comunitario. Curiosamente, è stato lo stesso Commissario per gli Affari Interni Cecilia Malmström, cioè l'equivalente del Ministro dell'Interno, a rendere nota la decisione a seguito delle risposte dei singoli Stati, affermando testualmente: *"At present there is no evidence, in terms of benefits for criminal investigation or the smooth functioning of the internal market of any need for a common EU approach in this area"*[2]. Non si tratta quindi di un minor interesse dell'UE in materia, ma di una presa d'atto delle valutazioni espresse dai Paesi in ordine ai riferiti minori benefici ai fini delle indagini apportati dalla implementazione delle misure di identificazione.

Considerata la situazione, non si può non prendere atto che utilizzare una SIM anonima senza presentare documenti falsi o contraffatti non solo è estremamente facile, ma perfettamente lecito in 16 Paesi Europei, senza bisogno di cercare in Rete gli innumerevoli siti che vendono SIM attive con traffico prepagato, documenti di identità e quant'altro.

Il problema forse deve necessariamente essere inquadrato anche sotto una prospettiva diversa, magari più ampia. L'acquisizione delle anagrafiche ai fini di sicurezza non è un problema di indagini, che indubbiamente esiste considerato che il crimine ha acquisito da tempo una dimensione transnazionale, ma di uniformità normativa. Ed è questo il punto sul quale il legislatore europeo dovrebbe porre la sua attenzione.©

NOTE

1. La direttiva sulla conservazione dei dati ha per obiettivo principale l'armonizzazione delle disposizioni degli Stati membri sulla conservazione di determinati dati generati o trattati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione. Essa è quindi volta a garantire la disponibilità di tali dati a fini di indagine, accertamento e perseguimento di reati gravi, come in particolare i reati legati alla criminalità organizzata e al terrorismo. In tal senso, la direttiva dispone che i suddetti fornitori debbano conservare i dati relativi al traffico, i dati relativi all'ubicazione nonché i dati connessi necessari per identificare l'abbonato o l'utente. La direttiva non autorizza, invece, la conservazione del contenuto della comunicazione e delle informazioni consultate.
   La High Court (Alta Corte, Irlanda) nonché il Verfassungsgerichtshof (Corte costituzionale, Austria) hanno chiesto alla Corte di Giustizia di esaminare la validità della direttiva, segnatamente alla luce di due diritti fondamentali garantiti dalla Carta dei diritti fondamentali dell'Unione Europea, ossia il diritto al rispetto della vita privata e il diritto alla protezione dei dati di carattere personale.
   Con la sua sentenza, la Corte ha dichiarato la direttiva invalida. La Corte ha rilevato anzitutto, che i dati da conservare consentono, in particolare,
   1) di sapere con quale persona e con quale mezzo un abbonato o un utente registrato ha comunicato,
   2) di determinare il momento della comunicazione nonché il luogo da cui ha avuto origine e
   3) di conoscere la frequenza delle comunicazioni dell'abbonato o dell'utente registrato con determinate persone in uno specifico periodo.
   La Corte ha ritenuto che la direttiva, imponendo la conservazione di tali dati e consentendovi l'accesso alle autorità nazionali competenti, si ingerisca in modo particolarmente grave nei i diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale. Inoltre, il fatto che la conservazione ed il successivo utilizzo dei dati avvengano senzache l'abbonato o l'utente registratone siano informati può ingenerare negli interessati la sensazione che la loro vita privata sia oggetto di costante sorveglianza.
   La Corte è passato poi ad esaminare se un'ingerenza siffatta nei diritti fondamentali in questione sia giustificata. Essa constata che la conservazione dei dati imposta dalla direttiva non è idonea ad arrecare pregiudizio al contenuto essenziale dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale. Infatti, la direttiva non consente di prendere conoscenza del contenuto delle comunicazioni elettroniche in quanto tale e prevede che i fornitori di servizi o di reti debbano rispettare determinati principi di protezione e di sicurezza dei dati. Inoltre, la conservazione dei dati i fini della loro eventuale trasmissione alle autorità nazionali competenti risponde effettivamente a un obiettivo di interesse generale, vale a dire la lotta alla criminalità grave nonché, in definitiva, la pubblica sicurezza.
   Tuttavia, la Corte ha ritenuto che il legislatore dell'Unione, con l'adozione della direttiva sulla conservazione dei dati, abbia ecceduto i limiti imposti dal rispetto del principio di proporzionalità
   (Fonte: Corte di giustizia dell'Unione europea COMUNICATO STAMPA n.54/14 Lussemburgo, 8 aprile 2014, www.curia.europa.eu)
2. Cfr pag. 10 di http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf ◊