ESAURIMENTO DEGLI INDIRIZZI IPV4 ED OBBLIGHI D'IDENTIFICAZIONE DEGLI UTENTI

di Marzia Minozzi

La normativa primaria in tema di conservazione dei dati delle comunicazioni, il d. lgs. 109/08, ha previsto che l'Operatore di telecomunicazioni debba conservare i dati relativi agli accessi internet attraverso la propria rete, tra cui l'indirizzo di protocollo internet (IP) univocamente assegnato. Allo stato attuale è stato raggiunto il limite fisico alla creazione di indirizzi IPv4. Tale situazione ha potenziali impatti sull'interpretazione della normativa citata. Inoltre, nell'ipotesi di utilizzo delle tecniche NAT per ovviare al limite raggiunto, l'identificazione diretta ed univoca dell'utente per il solo tramite dell'indirizzo pubblico IPv4, da questo utilizzato nel corso della connessione alla rete, diventa tecnicamente impossibile.

Lo sviluppo dei servizi Internet ed il conseguente fortissimo incremento della domanda di servizi di accesso alla rete hanno spinto gli Operatori di comunicazioni elettroniche italiani, per il tramite dell'Associazione di categoria, a sollevare da tempo il problema dell'esaurimento degli indirizzi IPv4[(1)], **per richiedere agli attori istituzionali la condivisione di problematiche e soluzioni tecniche e proporsi in ottica collaborativa**, verso quegli attori che potranno essere influenzati nella proprie pratiche correnti dall'utilizzo di tali soluzioni.
Gli indirizzi IP sono elementi della comunicazione che consentono l'individuazione dei punti di accesso alla rete; si tratta di una stringa numerica identificativa del punto su cui termina o da cui origina una comunicazione su Internet (una connessione). Gli indirizzi IP sono rilasciati e regolamentati dall'ICANN (*Internet Corporation for Assigned Names and Numbers*) tramite una serie di organizzazioni delegate, che passa per la IANA (*Internet Assigned Numbers Authority*) e, per l'Europa, dal RIPE NCC (Reti IP Europee – *Network Coordination Center*). È attualmente in uso la versione 4 (IPv4).

Esiste un limite fisico alla creazione di indirizzi IPv4, che è ormai stato raggiunto[(2)]: gli ultimi cinque blocchi di indirizzi IPV4 sono stati assegnati dallo IANA il 3 Febbraio 2011. A livello europeo la disponibilità si è esaurita a settembre 2012 ed il RIPE NCC non distribuisce più indirizzi IPv4 significativi al fine di offrire il servizio di connettività agli utenti finali italiani.
A livello mondiale, una soluzione di sistema, che consenta di preservare il funzionamento della rete nonostante tale esaurimento, è stata già individuata con la standardizzazione della versione 6 del protocollo IP, ovvero con il passaggio del sistema di indirizzamento da IPv4 a IPv6. Poiché è condivisa la consapevolezza che la transizione da IPv4 a IPv6 sarà un processo di medio/lungo termine (dai 5 ai 10 anni), sono state elaborate soluzioni per assicurare la coesistenza in rete di indirizzamento IPv4 e IPv6. Inoltre, per assicurare comunque la disponibilità di una numerosità di indirizzi IPv4 adeguata a garantire la piena funzionalità della rete, la IETF (*Internet Engineering Task Force*) ha raccomandato[(3)] una soluzione transitoria, individuata nell'utilizzo, sulle reti di accesso, delle tecniche di *Network Address Translation* (c.d. NAT).

Con tale tecnica, il gestore della rete di accesso attribuisce all'utente che si collega ad Internet, un indirizzo IP privato, univoco nella connessione richiesta, a sua volta correlato ad un indirizzo IP pubblico, che è l'unico ad essere visibile in rete e che viene assegnato contemporaneamente a più connessioni.

Nel periodo di transizione da IPv4 ad IPv6 potranno quindi essere utilizzati indirizzi IPv4 ("univocamente assegnati" come avviene attualmente), indirizzi IPv4 sottoposti a tecnica NAT (cosiddetti "nattati") e indirizzi IPv6. Poiché il protocollo IPv6 ed il protocollo IPv4 non sono nativamente intercomunicanti, finché il protocollo IPv6 non avrà raggiunto una diffusione di massa sul mercato mondiale, sarà necessario che gli utenti possano operare con indirizzi IPv4 al fine di mantenere la possibilità di navigazione telematica. Pertanto, considerata la scarsità di indirizzi IPV4 e la capacità di multiplazione delle tecniche di NAT, solamente attraverso tali tecniche sarà possibile avere un'adeguata disponibilità di indirizzi.
L'utilizzo di tali tecniche fa venire meno la corrispondenza biunivoca tra indirizzo IPv4 pubblico utilizzato per realizzare la connessione e utente intestatario della linea da cui origina la connessione. La stessa raccomandazione IEFT suggerisce quindi di tenere traccia della porta sorgente della comunicazione[(4)]. Associando all'indirizzo IPv4 pubblico la porta sorgente della comunicazione sarà sempre possibile conoscere univocamente le connessioni attivate; non sarà invece possibile risalire univocamente all'utente a partire dai soli dati della connessione, a meno che tra questi non vengano inseriti anche quelli relativi alla porta sorgente.
La conservazione dell'informazione sulla porta sorgente non è obbligatoria nei *records* di navigazione, tuttavia, essendo la memorizzazione della porta sorgente un elemento raccomandato dall'IETF, è pratica ormai adottata dai principali fornitori di servizi online (ad es. Google o Facebook) ed è ragionevole attendersi che tale dato sarà disponibile in misura crescente.

La situazione descritta sinora ha potenziali impatti sull'interpretazione della normativa primaria in tema di conservazione dei dati delle comunicazioni a fini di giustizia; infatti, il d. lgs. 109/08[(5)] ha previsto che l'Operatore di rete debba con-

servare i dati relativi agli accessi Internet attraverso la propria infrastruttura, tra cui l'indirizzo di protocollo internet (IP) univocamente assegnato, definito come "indirizzo di protocollo (IP) che consente l'identificazione diretta dell'abbonato o utente che effettua comunicazioni sulla rete pubblica".
È opportuno notare che:

(i) il conseguente obbligo di identificazione univoca di un determinato utente, per il tramite dell'indirizzo IP assegnato alla singola connessione generata dall'utente, è ulteriore rispetto a quanto previsto nella direttiva comunitaria recepita con il d. lgs. 109/08;

(ii) nell'ipotesi di utilizzo delle tecniche NAT (necessario per quanto detto sopra), l'identificazione diretta ed univoca dell'utente per il solo tramite dell'indirizzo pubblico IPv4 da questo utilizzato nel corso della connessione alla rete diventa tecnicamente impossibile. L'identificazione dell'utente rimane invece possibile associando all'indirizzo pubblico IPv4 l'ulteriore parametro di identificazione costituito dalla porta sorgente della comunicazione.

Al fine di mantenere la possibilità di identificare l'utente anche utilizzando tecniche NAT, si potrebbe pensare di ricorrere all'altro parametro di connessione, costituito dall'IP di destinazione, dato la cui conservazione è però illecita. L'indirizzo di destinazione (sia IP che URL) non è stato incluso tra i dati il cui mantenimento è autorizzato per finalità di giustizia ed inoltre è stato equiparato, dal provvedimento del 10 gennaio 2008 del Garante per la protezione dei dati personali, al contenuto della comunicazione. Rileva in proposito il Garante che "*alcuni dati di traffico telematico, apparentemente 'esterni' alla comunicazione elettronica (come, ad esempio, le pagine web visitate o gli indirizzi IP di destinazione), coincidono di fatto, nella maggior parte dei casi, con il 'contenuto' della comunicazione medesima, consentendo, tra l'altro, di ricostruire direttamente o indirettamente relazioni personali o sociali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute*". Pertanto, agli Operatori di reti telematiche è fatto divieto di effettuare ogni trattamento di dati personali consistente nella "*raccolta e conservazione, in qualsiasi forma e grado di dettaglio, di informazioni sui siti visitati dagli utenti, anche quando esse siano specificate con notazione URL o con mero indirizzo IP di destinazione*".
La memorizzazione ed il conseguente trattamento dell'indirizzo IP di destinazione di tutte le connessioni realizzate dagli utenti con indirizzo IPv4 "nattato" costituirebbero quindi una sorta di "intercettazione preventiva" delle comunicazioni di tali utenti, misura difficilmente compatibile con le norme generali dell'ordinamento. Peraltro, l'associazione indirizzo IPv4/IP di destinazione rischia comunque di non condurre ad un risultato univoco di identificazione dell'utente nel caso di siti molto frequentati (*social networks* o di motori di ricerca); si rischierebbe così di ingenerare falsi affidamenti sui risultati delle identificazioni stesse. **La soluzione che prevede la conservazione, ai fini di giustizia, dell'associazione di indirizzo IPv4 pubblico e indirizzo IP di destinazione appare quindi non percorribile sotto il profilo giuridico e non soddisfacente sotto quello operativo**.
L'interpretazione del vigente dettato normativo deve avere riguardo alla necessaria evoluzione delle tecniche di connessione, altrimenti gli Operatori si troveranno obbligati non all'identificazione univoca dell'utente in base all'indirizzo IPv4 pubblico, ormai impossibile, ma alla **cessazione del servizio**, ipotesi (evidentemente) impraticabile, anche alla luce della natura di pubblica utilità del servizio in questione.
Gli Operatori nazionali si trovano costretti ad adottare le tecniche di NAT e, allo stato della normativa vigente, le prestazioni obbligatorie di giustizia possono essere eseguite solamente ricorrendo all'associazione degli indirizzi IPv4 alla porta sorgente; una misura di mitigazione degli effetti indesiderati di tale adozione può essere la preassegnazione delle porte, che - per dati intervalli del valore di porta sorgente - ristabilisce la relazione biunivoca tra indirizzo pubblico IPv4 e utente che effettua la connessione. Ulteriori accorgimenti in grado di minimizzare gli effetti sulle pratiche di indagine attualmente in uso sono ampiamente possibili e passano, ad esempio, da una diversa gestione della variabile temporale delle interrogazioni rivolte ai gestori. Come per tutte le innovazioni tecniche, sarà necessario un primo periodo di osservazione dei risultati reali del loro funzionamento e la migliore collaborazione possibile tra autorità inquirenti ed Operatori al fine di comprendere e risolvere le rispettive criticità.
Allo stato attuale, invece, la possibilità che interpretazioni della norma particolarmente restrittive provochino problemi agli Operatori complica il contesto in cui questi si trovano ad agire e a interagire con i referenti istituzionali, che sono molteplici. Infatti, in questa materia esprimono interessi, a volte non completamente compatibili, l' Autorità Giudiziaria e quella inquirente, il Garante per la tutela dei dati personali, il Ministero per lo Sviluppo Economico.
Sinora, dal complesso di questi soggetti non sono giunte agli Operatori tutte le rassicurazioni richieste rispetto alla condivisione di tutto quanto esposto sinora, forse in una sottovalutazione del problema. Appare invece necessario addivenire in tempi rapidi ad una esplicita condivisione della situazione, che vada nella direzione appena illustrata, per dare agli Operatori la necessaria certezza del quadro normativo e relazionale in cui adottare improcrastinabili decisioni di investimento e per consentire loro una piena collaborazione con tutti i soggetti interessati alla minimizzazione degli effetti meno desiderabili connessi all'adozione delle tecniche NAT.
In tal senso, un intervento prioritario nell'agenda del prossimo Parlamento sarebbe una interpretazione autentica del d. lgs. 109/08, laddove tratta di identificazione univoca diretta dell'utente a partire dal suo indirizzo IPv4 pubblico. ©

NOTE

1. L'indirizzo IPv4 è costituito da 32 bit (4 byte) suddiviso in 4 gruppi da 8 bit (1 byte). Ciascuno di questi 4 byte è poi convertito in formato decimale di più facile identificazione. Un esempio di indirizzo IPv4 è 195.24.65.215.
2. Oltre 4 miliardi di indirizzi.
3. RFC6302- *Logging Recommendations for Internet-Facing Servers.*
4. Le porte sono numeri utilizzati per identificare una particolare connessione di trasporto tra quelle attive su un calcolatore; la porta sorgente è assegnata casualmente in maniera tale da identificare univocamente la connessione da parte del mittente col destinatario, eventualmente tra più *computers*.
5. Il d. lgs 109/08 ha recepito la direttiva 2006/24/CE riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione (c.d. direttiva Frattini). ◊