Lawful Interception Academy (LIA)

Atti dell'edizione 2014 della LIA svoltasi a Roma dal 17 al 21 novembre 2014 presso la Scuola di Formazione del Corpo di Polizia Penitenziaria intitolata a "Giovanni Falcone". La Lawful Interception Academy, è un corso di alta formazione per addetti della Pubblica Amministrazione che sono professionalmente impegnati negli ambiti di utilizzo e di analisi dei risultati provenienti dagli strumenti utilizzati oggi per le indagini e per la ricerca della prova, relativamente alle vecchie e nuove tecnologie di comunicazione. La LIA è stata fondata dalla rivista "Sicurezza e Giustizia" e rappresenta il passaggio in "aula" dell'attività didattica svolta dalla rivista su "carta" negli anni. La LIA è destinata esclusivamente ad appartenenti della PA ed è per questi gratuita, seguendo la stessa impostazione della rivista. La LIA si avvale dei più moderni sistemi di mobile learning.

di Donatella Proto

ESAURIMENTO DEGLI INDIRIZZI IP ED OBBLIGHI DI IDENTIFICAZIONE DEGLI UTENTI

***Donatella PROTO** è Dirigente della Divisione 1 del MISE "Reti e Servizi di comunicazione elettronica ad uso pubblico della Direzione Generale per i servizi di comunicazione elettronica, di radiodiffusione e postali". Componente dell'Osservatorio per la sicurezza delle reti e delle comunicazioni di cui al decreto del 14 gennaio 2003, come modificato dal decreto dell'5 settembre 2010.*

1. La risorsa IPV4 : la sua allocazione e il suo esaurimento

Ogni apparecchiatura connessa ad Internet per funzionare deve utilizzare un indirizzo per ciascuna delle interfacce di rete: per es. un PC che utilizza contemporaneamente la rete *wired*, il *wifi* ed una chiavetta 3G avrà almeno tre indirizzi distinti, *che dovrebbero essere univoci*. All'assegnazione degli indirizzi IP provvedono enti – senza scopo di lucro – preposti alla *Governance* di Internet: per l'area europea tale ente è il RIPE Ncc. Dal 1983 su Internet è operativa la versione 4 del Protocollo IP (IPV4), ove per protocollo IP si intende l'insieme delle regole che regolano il trasporto dei dati sulla rete. La versione 4 dell'Internet Protocol, cioè l'IPV4, usa indirizzi costituiti da 32 bit, suddivisi in n 4 gruppi da 8 bit, separati ciascuno da un punto, ad es.:

11111111.11111111.11111111.11111111

La struttura dell'indirizzo IPV4 rende evidente come gli indirizzi non possono bastare per tutti: in ciascun Paese non potrebbero essere assegnati a più di 16 milioni di dispositivi, nel mondo a non più di 4 miliardi. **Oggi per l'accesso alla rete vengono utilizzati 2,9 miliardi di indirizzi IPV4, di cui circa 50 milioni assegnati in Italia anche a settori che nulla a che fare con il mondo delle telecomunicazioni**, sebbene si tratti di una risorsa scarsa e strategica. Circa il 10% delle risorse IPV4 è al momento utilizzato per scopi avulsi dai servizi tlc, come media, industria e pubblica amministrazione: un'inutile accaparramento o meglio una speculazione alimentata dalla scarsità degli indirizzi attualmente disponibili e derivante da un non corretto sistema di Governance. Una risorsa scarsa e strategica dovrebbe essere assegnata in modo trasparente e preciso ed essere utilizzata in modo efficiente – come per le numerazioni telefoniche o le frequenze – in modo tale che le amministrazioni preposte alla sorveglianza sul mercato possano svolgere in modo efficace il proprio compito, considerando che l'accaparramento degli indirizzi IPV4 può generare di per sè una posizione dominante ed una barriera all'accesso ai mercati dei servizi tlc.

Fino ad oggi gli indirizzi IPV4 sono stati assegnati sul base del principio "*first came first served*" e **dal 2012**, a seguito del repentino esaurimento degli indirizzi IPV4 in concomitanza con lo sviluppo della società dell'informazione e l'aumento dei dispositivi connessi, **non vengono più assegnati nuovi indirizzi IPV4**. Ciò ha favorito l'insorgere di un mercato parallelo avulso da qualsiasi controllo ed indirizzo: è bene tener presente, infatti, che se un indirizzo è assegnato non vuol dire che sia effettivamente utilizzato. **Un indirizzo IP per essere raggiungile deve essere "annunciato" in rete: il 4% degli indirizzi IP assegnati all'Italia "non è annunciato" e di questi circa 1 milione riguarda il settore tlc**.

2. La risorsa IPV6: una transizione non facile verso una soluzione … ora solo di nicchia

All'approssimarsi dell'esaurimento degli indirizzi IPV4 in ambito internazionale si è scelto di allargare le capacità di indirizzamento passando all'IPV6. L'indirizzo IPV6 è costituito da 128 bit, suddiviso in 8 gruppi di 4 numeri esadecimali che rappresentano 2 byte ciascuno separati da due punti. È stato ampliato l'arco di numerazione da 4 a 16 ottetti e, quindi, lo spazio di indirizzamento.

La transizione verso l'IPV6 non sarà così rapida, in quanto l'indirizzamento IPV4 non è direttamente compatibile con quello IPV6 ed anzi la mancanza di vincoli e scadenze ha contribuito a far considerare di bassa priorità tutti gli interventi finalizzati all'attivazione dell'IPV6, conseguenza anch'essa di una non corretta Governance di Internet. Sarebbe, infatti, stato auspicabile un ruolo attivo dei "Governi", che favorisse la conoscenza del nuovo protocollo e, quindi, la domanda: difficilmente i vantaggi derivanti dall'adozione del nuovo protocollo potranno essere evidenti se la nuova versione rimane una soluzione di nicchia.

La migrazione IPV6 implica, infatti, la totale (ed impossibile) migrazione di tutte le risorse che utilizzano Internet ad una nuova tecnologia per cui:

— tutti gli apparati in circolazione devono essere in grado di gestire l'indirizzo IPV6: si consideri, invece, che il 90% dei terminali mobili attualmente sul mercato sono configurati su IPV4 e solo un piccolo sottoinsieme prevede l'opzione di configurazione IPV6 (e peraltro non *Over The Air*) e se il settore della larga banda mobile sicuramente è il settore a maggior tasso di sviluppo è anche il settore a maggior tasso di consumo di indirizzi IP, e, peraltro, con un trend di crescita delle utenze mobili *IP-always-on*;
— tutte le reti devono essere in grado di assegnare indirizzi IPV6: nessuno grande operatore di rete europeo (tra cui sono da annoverare quelli che in virtù dell'accaparramento di indirizzi IPV4 hanno conquistano una posizione dominante) è in grado di garantire la navigazione con protocollo IPV6 e, se è vero che i grandi *content provider* americani (come Google, Facebook, Yahoo) consentono la navigazione con protocollo IPV6, non è detto che la navigazione avvenga con tale protocollo, se il sistema operativo del *computer* o del terminale, il *modem* o la chiavetta non sono abilitati all'IPV6;
— tutte le applicazioni client, web e server devono essere in grado di operare in IPV6;
— tutti gli utilizzatori devono aggiornare – ove possibile - i lori HW e cambiare i loro SW operanti in IPV4, spesso manualmente, per cui è probabile che il cliente non si adoperi per modificare le impostazioni di origine, sia per possibile mancanza di competenza tecnica e sia per mancanza di uno specifico vantaggio in termini di qualità del servizio.

Infine, il valore degli indirizzi IPV4 è stimato in circa 30 miliardi di dollari e si consideri anche che l'attivazione dell'IPV6 comporta la riprogettazione dei meccanismi di protezione delle reti e la riorganizzazione dei servizi di assistenza ai clienti e di *billing*. **Il passaggio dall'IPV4 all'IPV6 appare, quindi, essere un processo complesso, di scala sovranazionale in quanto deve coinvolgere l'intero ecosistema di Internet** (siti, terminali, CPE …..), costoso ed apparentemente nel breve periodo non vantaggioso.
Sebbene, infatti, ci siano grandi utenti ai quali gli operatori forniscono connettività IPV6 o che hanno avviato programmi di adeguamento delle loro reti (vedasi nel mondo universitario l'operato del consorzio GARR ma anche nell'ambito della pubblica amministrazione l'operato per es. del Comune di San Benedetto del Tronto) tale azione non risolve il problema dell'esaurimento degli indirizzi IPV4 dal momento che si pone comunque il problema di garantire la raggiungibilità di destinazioni IPV4 almeno per i prossimi 5/10 anni e di soddisfare utenti che continuano a richiedere indirizzi IPV4.

Al di là degli esempi sopracitati ed altri casi di eccellenza, soprattutto nell'ambito della pubblica amministrazione, il traffico in IPV6 costituisce oggi una frazione assolutamente trascurabile rispetto al traffico totale (solo l'1% secondo i rilevamenti di Google) ed, inoltre, il sistema di connettività pubblica è basato sull'IPV4, così come sono raggiungibili solo ed esclusivamente in IPV4 i siti ufficiali delle amministrazioni centrali ("…..gov.it"), **per cui è evidente ed inevitabile che si è in un periodo di transizione,** nel quale appare rilevante non solo il ruolo dei produttori e dei consumatori, ma anche e sopratutto il ruolo che i Governi vorranno assumere nella gestione di tale periodo al fine di evitare il blocco del settore ed il passaggio al nuovo protocollo.

In tale periodo di transizione, se da un lato va sostenuto il processo di adozione del nuovo protocollo, dall'altro, infatti, non può non essere garantita e favorita la compatibilità tra i due sistemi senza richiedere eccessivi investimenti, ma ristabilendo adeguate condizioni di sviluppo e di sicurezza, senza pregiudizio per le indagini e per la privacy (considerando che i servizi di interconnessione IPV6- IPV4 per definizione sono posti all'estero). La doppia raggiungibilità non è un problema tecnico in quanto sul mercato esistono soluzioni che consentono l'utilizzo temporaneo dei due protocolli (soluzioni cd *dual stack*) e consentono di gestire le richieste di connessioni su entrambi i tipi di rete, ma tali soluzioni necessitano, comunque, dell'utilizzo di un indirizzo IPV4.

Quale la possibile soluzione per evitare un degrado della *user experience* in termini di tempo di connessione o l'improbabile interruzione dei servizi di connessione alla rete con tutte l conseguenze facilmente immaginabili sull'attuazione dell'Agenda Digitale Europea 2020?
L'unica soluzione efficacemente perseguibile nell'interesse dello sviluppo del Paese e delle imprese è l'utilizzo di tecnologie di traduzione degli indirizzi di rete "uno a molti": le cd *Network Address Traslation* (NAT) tecniche che consentono agli operatori di continuare a fornire servizi ai nuovi clienti e permettono al mondo IPV6 di interoperare con il mondo IPV4.

Il principio di funzionamento del NAT è lo stesso sia nel caso di rete fissa che di rete mobile e consiste in una tecnica che effettua la traduzione da indirizzo privato ad indirizzo pubblico e viceversa, nel momento in cui il cliente naviga in Internet. Questo significa che diversi clienti utilizzano lo stesso indirizzo IP pubblico per la sessione di navigazione: il parametro N (cioè il numero dei clienti che utilizzano lo stesso indirizzo) varia a seconda dell'operatore, della propria disponibilità di indirizzi pubblici e della domanda di connettività che deve soddisfare.

Tale soluzione comporta l'impossibilità di identificare in modo univoco gli utilizzatori di un determinato indirizzo IP, dando la possibilità di commettere abusi sulla rete, essendo possibile per l'operatore indicare esclusivamente la rosa dei nominativi degli utenti che alla data ed all'ora indicata hanno utilizzato l'indirizzo IP oggetto della richiesta: **in Italia il combinato disposto dall'art. 96 del Codice delle comunicazioni elettriche e del decreto legislativo n. 109/2008 – cd Decreto Frattini – vieta (ora) tale possibilità**.

3. L'attuale quadro normativo e le possibili soluzioni al problema dell'esaurimento degli indirizzi IPV4

Tra le prestazioni di giustizia di cui al sopracitato art. 96 vi è l'obbligo per gli operatori di identificare la linea chiamante o connessa. Il cd decreto Frattini impone all'operatore l'obbligo di conservare i dati relativi agli accessi ad Internet attraverso la propria rete per dodici mesi dalla data di comunicazione – esclusi i contenuti della comunicazione – per finalità di accertamento e repressione dei reati e tra questi dati vi sono "*… il nome e l'indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati univocamente assegnati l'indirizzo di protocollo Internet, un identificativo di utente o un numero telefonico …..*". Il decreto definisce, altresì, il concetto di "***indirizzo di protocollo internet univocamente assegnato come l'indirizzo di protocollo che consente l'identificazione diretta dell'abbonato o dell'utente che effettua comunicazioni sulla rete pubblica***".

Quali le possibili soluzioni per affrontare il problema dell'esaurimento degli indirizzi IPV4 in Italia, stante l'attuale quadro normativo e le improbabilità di applicare le previste sanzioni? Le problematiche di esaurimento degli indirizzi IPV4 e la transizione all'IPV6 sono da tempo oggetto di approfondimento anche nell'ambito dell'Osservatorio per la sicurezza delle reti e delle comunicazioni, istituito presso il Ministero dello sviluppo economico con Decreto interministeriale dell' 8 settembre 2010.
Per chiarezza di esposizione è bene, tuttavia, tenere distinte le problematiche giuridiche derivanti dall'esaurimento degli indirizzi IPV4 ed i motivi essenzialmente tecnico-economici del ritardo dell'IPV6, sebbene strettamente correlati.

Il problema dell'esaurimento degli indirizzi IPV4, stante la mancata transizione all'IPV6, **ha creato un'antinomia tutta italiana, in quanto vede contrapposte le esigenze di sicurezza e di investigazione delle forze di polizia alle esigenze di mercato degli operatori di comunicazione derivanti dall'aumento della domanda di connessioni ad Internet,** nel rispetto delle norme in materia di tutela dei dati personali. La contrapposizione tra due priorità per il Paese (da un lato l'incentivazione dell'accesso ad Internet per l'abbattimento del *Digital Divide* e dall'altra la sicurezza del Paese) nasce dalla necessità degli operatori di dover rispettare le stringenti disposizioni di cui al decreto legislativo n. 109/2008 (cd decreto Frattini), dell'art. 96 del Codice delle comunicazioni (Dlgs. n. 259/2003) in tema di prestazioni obbligatorie e le disposizioni dettate dal Garante della privacy in tema di tempi e modalità di conservazione dei dati di traffico telematico (art. 132 del Dlgs. n. 196/2003).

A fronte dell'esaurimento degli indirizzi IPV4 e della non immediata adozione dello standard IPV6 **vi è, infatti, oggi l'impossibilità per gli operatori di garantire l'univocità nell'identificazione dell'utente**, così come prescritto dalla citata normativa.
Nell'ambito del citato Osservatorio per la sicurezza delle reti e delle comunicazioni si è tentato di condividere un'ipotesi di modifica del suddetto decreto Frattini che a fronte dell'indisponibilità di indirizzi univoci prevedesse la conservazione o dei *log* di destinazione o della porta sorgente delle comunicazioni oggetto dell'indagine, che associata all'IP di partenza, alla data ed ora della connessione consentirebbe di individuare – in modo univoco - tra gli utilizzatori del medesimo indirizzo IP l'utente desiderato. Ma entrambe tali soluzioni non sono state ritenute condivisibili: **la porta sorgente non è un parametro di cui si tiene sempre traccia nelle comunicazioni via Internet** (è un obbligo che dovrebbe/potrebbe essere imposto agli operatori di destinazione ed ai cd *content provider* anche se esteri, considerando che verso quest'ultimi è indirizzata la gran parte del traffico nazionale) **e l'indirizzo di destinazione è stato equiparato dal Garante della privacy al contenuto della comunicazione con un provvedimento del 10 gennaio 2008**. Inoltre il *logging* dell'IP di destinazione sotto il profilo tecnico non garantisce la certa identificazione dell'utente: qualora più utenti si connettano allo stesso sito non è da escludere che nello stesso istante di tempo si possa verificare l'utilizzo della stessa accoppiata IP pubblico + *log* di destinazione. Sotto il profilo della ragionevolezza e proporzionalità dell'intervento entrambe le soluzioni portano, inoltre, ad un aumento esponenziale delle informazioni da memorizzare con conseguenti significativi impatti economici per gli operatori.

Ed allora quale la possibile soluzione?
Il punto nodale è l'applicazione del decreto legislativo n.109/2008, attuativo della direttiva 2006/24/CE, riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione: è necessario intervenire per adeguare la disciplina prevista dal predetto decreto legislativo all'evoluzione tecnologica della rete internet.

La formulazione attuale del citato decreto legislativo stabilisce una relazione univoca tra utente della connessione e indirizzo IP pubblico assegnato alle sessioni di navigazione su Internet, che deve essere rivalutata: tale relazione non è, infatti, prevista nella direttiva comunitaria, che adotta definizioni più generiche di quelle presenti nella norma nazionale e che è stata ad es. recepita in Francia, Spagna e Regno Unito senza alcuna prescrizione in tema di assegnazione univoca dell'indirizzo IP per identificare l'utente. Anzi in Germania il diritto alla privacy è stato ritenuto prevalente rispetto alle esigenze di sicurezza, tanto da far dichiarare incostituzionale un obbligo di conservazione generalizzata dei dati in mancanza (quindi) di elementi di reato.

Alla luce dei tassi di crescita dell'utilizzo di apparati e servizi (*smartphone*, connessioni a banda larga e servizi *on-line*), che richiedono un crescente e più intensivo utilizzo degli indirizzi IPV4 da parte dell'utenza nazionale, appare, pertanto, necessario ed indifferibile un "intervento" (normativo?).
Il mantenimento dello *status quo* normativo e l'esaurimento degli indirizzi IPV4 condurrebbero, infatti, inevitabilmente, nel giro di pochi mesi, all'impossibilità di erogare il servizio di connettività ad Internet, **lasciando agli operatori del settore l'alternativa tra l'interruzione del servizio e il mancato rispetto del requisito della univocità di assegnazione dell'indirizzo IP con la contestazione di pesanti sanzioni**. L'art. 162 bis del Codice per la tutela dei dati personali (Dlgs n. 196/2003), così come modificato dall'art. 5 del Dlgs n. 109/2008, prevede che **nel caso di assegnazione di indirizzo IP che non consenta l'identificazione univoca dell'utente o dell'abbonato si applica la sanzione amministrativa pecuniaria da 5.000 a 50.000 euro che può essere aumentata fino al triplo in ragione delle condizioni economiche dei responsabili della violazione**.

Tali sanzioni non possono non essere archiviate per buona fede e causa di forza maggiore, avendo l'operatore considerato legittimo l'affidamento al sistema tecnologico utilizzato per l'assegnazione univoca degli indirizzi IP, in considerazione dell'obiettiva situazione di incertezza esistente, escludendosi ogni addebito sotto il profilo soggettivo rispetto alla condotta posta in essere dall'operatore medesimo.

4. La soluzione Carrier Grade NAT o Port Block Allocation (PBA) o Deterministic NAT

Una possibile soluzione in realtà esiste: un efficiente e praticabile utilizzo degli strumenti di NAT potrebbe essere non l'uno a molti ma l'uno ad un insieme molto ridotto, misurato in termini di massimo "Rapporto di condivisione" e cioè numero massimo di utenti che possono contemporaneamente condividere lo stesso indirizzo IPV4, imponendo un limite numerico e temporale a tale rapporto di condivisione e diversificandolo tra reti fisse e reti mobili. Esistono (o *rectius* esistevano) significative differenze nel servizio di accesso ad Internet tra le reti fisse e le reti mobili, ove le reti fisse sono caratterizzate da una rigida e stabile connessione tra utente e rete e da una maggiore quantità di servizi Ip acceduti contemporaneamente per singolo utente, mentre le reti mobili sono caratterizzate dalle inevitabili inefficienze dell'accesso mobile e da una minore quantità di servizi acceduti contemporaneamente per singolo utente, sebbene tale distinzione si stia affievolendo, dato che molte APP e servizi erogati sulla rete mobile operano come nel caso delle reti fisse in modalità *IP-always-on* cioè con connessioni permanenti.

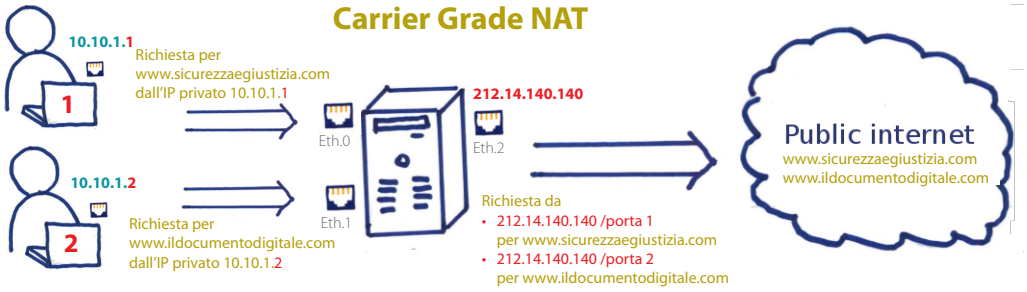

Figura 1 - Schema semplificato del NAT con utilizzo di porte sorgente che l'ISP dovrebbe tracciare.

Allo scopo di trovare una soluzione a quello che, come detto, è un'antinomia tutta italiana, agli inizi del 2014 l'Osservatorio per la sicurezza delle reti e delle comunicazioni ha fatto un'indagine tra gli operatori nazionali per conoscere il massimo "rapporto di condivisione" degli indirizzi IPV4 ritenuto necessario per garantire il servizio pubblico sulla propria rete e congruo rispetto al tasso di contemporaneità e cioè al massimo numero di utilizzatori che nello stesso periodo temporale richiedono l'accesso ad internet. Nella determinazione del massimo rapporto di condivisione possibile è necessario tener presente che tale tasso di contemporaneità è destinato inevitabilmente a crescere con il diffondersi degli *smartphone* e dei servizi legati all'Internet delle cose (come i servizi M2M). Il *trend* di crescita degli accessi contemporanei ad Internet nel 2013 è stato pari al 30% ed è destinato a salire negli anni addivenire.

Considerando il *trend* del tasso di contemporaneità e mutuando la soluzione *Carrier Grade Natting* adottata in altri Paesi europei (come ad es. in Belgio) **la soluzione al problema giuridico dell'esaurimento degli indirizzi IPV4 è di "riconoscerla" come valida anche in Italia mediante la rigida pre-assegnazione di blocchi di porte IP, talchè l'assegnazione dell'indirizzo IPV4 unito al blocco di porte risulti univoca**.
Le condizioni per l'utilizzazione del *Carrier Grade Natting* dovrebbero essere le seguenti:

— NAT con allocazione di blocchi di porte;
— diverso rapporto di condivisione per fisso e mobile: 1:8-1:16 per il fisso, 1:32-64 per il mobile;
— obbligo per gli ISP di tenere traccia della porta sorgente;
— registrazione del momento (data ed ora locale) in cui l'indirizzo viene allocato e del momento in cui viene de-allocato.

5. Conclusioni

È necessario ragionare su un piano nazionale di transizione all'IPV6, da approntare con la partecipazione dell'Agenzia per l'Italia Digitale, che coinvolga *in primis* il comparto governativo e della pubblica amministrazione, che preveda l'adozione di IPV6 sui siti del Governo e delle pubbliche amministrazioni e l'acquisto di beni e servizi da parte della pubblica amministrazione solo se IPV6 compatibili (sulla falsariga della posizione adottata dal governo spagnolo) e favorisca un rapido ricambio dell'elettronica di consumo.
Ma fin quando tutte le amministrazione coinvolte non interverranno è necessario tener presente che l'art. 96, comma 1, del citato Codice delle comunicazioni elettroniche stabilisce che "*i tempi e i modi*" delle prestazioni ai fini di giustizia "*sono concordati*" con le autorità giudiziarie da parte di ciascun Operatore. Un ausilio alla individuazione delle modalità con cui possono essere effettuate siffatte prestazioni può venire dal cd Listino in cui sono elencate le "caratteristiche" delle prestazioni da ritenersi obbligatorie per le diverse categorie di servizio offerto al pubblico, pubblicato sul S.O. della G.U. 7 maggio 2001 n.104 e, sebbene la categoria di fornitore di accesso ad Internet non figura tra le categorie del citato Listino, non per questo viene meno l'obbligo di collaborazione tra l'operatore e l'autorità giudiziaria.
La natura della prestazione obbligatoria in tal caso è individuabile per analogia con quelle imposte agli operatori di telefonia, fermo restando in ogni caso il rispetto delle norme sulla tutela dei dati personali e le disposizioni del Codice di procedura penale. In ogni caso l'operatore dovrà attenersi con la massima diligenza a quanto formalmente e motivatamente richiesto dall'AG mediante notifica dello specifico decreto in cui viene dettagliata l'attività di acquisizione (e/o di intercettazione). ©