Risposta alla Consultazione pubblica sulla neutralità della rete Agcom, delibera n. 40/11/CONS

Quesito 2.
Quali tipologie di servizi dati e quali forme di gestione del traffico assumono particolare rilievo nell'ambito del dibattito riguardante la neutralità della rete? Qual è il presumibile impatto che la crescente diffusione delle forme di gestione del traffico di rete per ragioni tecniche o di blocco di applicazioni per motivi commerciali avrà sul principio della neutralità della rete? Quali fattori concorrono alla declinazione della definizione di neutralità della rete?

1. Il concetto di gestione del traffico e una "nuova neutralità della rete"

Come sottolineato dal Body of European Regulators for Electronic Communications (BEREC), in risposta alla consultazione sulla neutralità della rete avviata dalla Commissione europea a giugno 2010, "l'uso della gestione del traffico [*traffic management*] non si qualifica di per sé come giusto o sbagliato. Questo dipende dagli obiettivi per cui è usato, le circostanze nel quale è usato e l'impatto sugli obiettivi generali (fra cui gli effetti sulla concorrenza, l'efficienza degli investimenti e l'apertura di internet)" (2010: 9).

All'interno di questo quadro, si rivela particolarmente utile il concetto di discriminazione di banda (*broadband discrimination*), sviluppato già nel 2003 da Tim Wu (2003). Secondo Wu, la discriminazione di banda può essere intesa come uno strumento per raggiungere un "nuovo" concetto di neutralità della rete, adeguato all'evoluzione di internet. Wu, in particolare, considera il concetto originario del protocollo TCP/IP come datato, in quanto questo protocollo era neutrale solo nei confronti di *data applications* (come l'invio di email o la normale navigazione sul web), per le quali il "fattore tempo" non era determinante.

Con l'evoluzione di internet e la diffusione di tecnologie sensibili al fattore tempo (*time-sensitive*) diviene quindi necessario rivedere l'applicazione del protocollo TCP/IP, dal momento che questo protocollo non è più *effettivamente neutrale* nei confronti di tutte le applicazioni, ma opera una discriminazione (o perlomeno crea uno svantaggio) nei confronti di quelle applicazioni come il VOIP o lo streaming video per le quali la simultaneità di ricezione è parte essenziale della loro stessa esistenza.

"In un universo di applicazioni che include applicazioni sensibili e insensibili al fattore tempo [*latency-sensitive and insensitive applications*] è difficile considerare il protocollo IP come veramente neutrale fra tutte le applicazioni" (Wu, 2003: 148).

La domanda cruciale seguente è: quali tipi di forme di gestione del traffico o di discriminazione di banda garantiscono il rispetto della nuova neutralità della rete, senza danneggiare la concorrenza del mercato o la protezione dei dati personali?

Davide Morisi – davidemorisi@gmail.com – www.davidemorisi.com

2. Diverse forme di gestione del traffico

Un elenco altamente esaustivo di forme di gestione del traffico viene fornito dalla stessa Agcom nella delibera n. 39/11/CONS. Vale la pena in questa sede, quindi, elencare solamente le forme attualmente più diffuse, in riferimento ad alcuni Internet service provider (ISP).

Secondo Ofcom, l'autorità garante per le comunicazioni nel Regno Unito, "è una pratica comune per alcuni ISP gestire la banda durante periodi di congestione o quando un gruppo di abbonati utilizza una quantità sproporzionata della capacità totale, a detrimento di altri utenti" (2010: 6).

Attualmente solo due ISP italiani non adottano alcuna forma di gestione del traffico:

- **Fastweb** e **Tiscali**[1]

Ne fanno uso invece tutti gli altri ISP italiani:

- **Telecom Italia**, **Infostrada**, **Vodafone** e **TeleTu**[2]

Nel Regno Unito tutti i maggiori ISP, senza eccezioni, adottano forme di gestione del traffico o *fair use policies* come dichiarato nei siti ufficiali:

- **BT, Virgin Media, Aol, Talk Talk, Orange**[3]

In generale, questi ISP utilizzano una modalità detta *traffic shaping*, per dare priorità a certi tipi di traffico in internet. Altre due forme comuni di gestione del traffico sono la *Content Distribution Networks* e la *ISP traffic prioritisation*, mentre una forma estrema di gestione è il *blocking*. (Per la spiegazione in dettaglio di queste varie forme di *traffic management* si rimanda alla delibera 39/11/CONS della Agcom e al documento di Ofcom, 2010.)

Un'altra particolare forma di gestione del traffico, infine, è la cosiddetta Deep Packet Inspection (DPI), "una tecnologia che consente ai pacchetti dati di essere gestiti a seconda del contenuto veicolato, piuttosto che semplicemente in base all'indirizzo IP sull'*header* del pacchetto" (Ofcom 2010: 63).

1 Fastweb, http://www.fastweb.it/offerte/velocita-internet/
Tiscali, http://abbonati.tiscali.it/documenti/delibera/pdf/Allegato_6_B2C_20M.pdf

2 Telecom Italia, http://www.telecomitalia.it/assistenza/info-consumatori/news-187/novit%C3%A0-gestione-servizi-adsl
Infostrada, http://www.infostrada.it/areaclienti/pls/portal30/w155.getpagexml?p_xml=liberorisponde/full63.phtml
Vodafone Italia,
http://www.areaaziende.vodafone.it/190/trilogy/jsp/programView.do?pageTypeId=9610&programId=12545&channelId=-8671&contentKey=48195&SR=2&SC=peer+to+peer
TeleTu, http://www.teletu.it/internet/offerte/adsl/adsl-senza-limiti.php

3 BT Broadband Fair Usage Policy, http://bt.custhelp.com/app/answers/detail/a_id/10495/c/346,402,424
Virgin Media Cable Traffic management policy,
http://help.virginmedia.com/system/selfservice.controller?CONFIGURATION=1002&PARTITION_ID=1&TIMEZONE_OFFSET=&USERTYPE=0&VM_CUSTOMER_TYPE=Cable&CMD=VIEW_ARTICLE&ARTICLE_ID=2781
Fair Use Policy for AOL Broadband,
http://help.aol.co.uk/help_uk/microsites/search.do?cmd=displayKC&docType=kc&externalId=uk_2264599212
Talk Talk Fair Usage Policy, http://www.talktalk.co.uk/legal/fup.html
Orange Fair Use Policy,
http://www.orange.co.uk/terms/7094.htm?linkfrom=terms_16353&link=link_7&article=termsofusenav

Davide Morisi – davidemorisi@gmail.com – www.davidemorisi.com

Quesito 3.
(…) Quali forme di gestione del traffico possono essere considerate ragionevoli?

3. Il concetto di "gestione ragionevole"

Come specificato dalla FCC (2010: 48), una pratica di gestione del traffico si può definire ragionevole se indirizzata ai seguenti obiettivi:

a) assicurare la sicurezza e l'integrità della rete;
b) gestire il traffico "non desiderato" in base alle scelte dell'utente (ad esempio il controllo dei genitori sul contenuto potenzialmente dannoso per i figli);
c) ridurre o mitigare gli effetti della congestione della rete.

Per esclusione, tutti gli altri possibili obiettivi sono dunque da ritenersi irragionevoli o illegittimi. È proprio in questo ambito che l'uso della DPI solleva una serie di problemi, in quanto permette agli ISP di perseguire una serie di obiettivi ben più ampia rispetto a quanto definito dalla FCC. Per questo motivo, come illustra l'analisi seguente, difficilmente questa forma di *traffic management* può considerarsi interamente ragionevole.

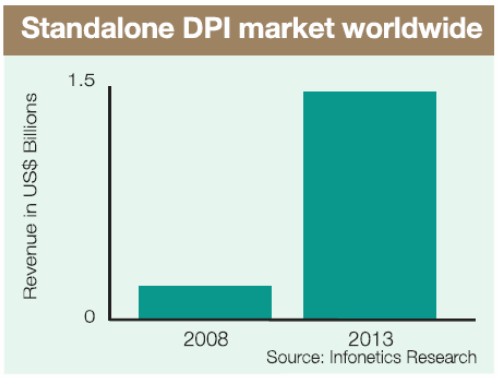
4. Deep Packet Inspection

4.1. Come funziona

La tecnologia DPI permette di analizzare tutti i sette livelli del modello OSI, giungendo al livello applicativo, ovvero il messaggio effettivamente inviato tramite internet. Questa potenzialità è evidenziata dai maggiori produttori internazionali di questi dispositivi: Ipoque[4], Procera[5] e Arbour Networks[6].

4.2. Un mercato in costante crescita

Secondo i dati forniti da Infonetics Research, se nel 2008 il mercato globale della Deep Packet Inspection valeva 207 milioni di dollari, nel 2013, secondo le previsioni, questa cifra raggiungerà il valore di 1,5 miliardi di dollari (Rubenstein, 2010: 14).



4 "PRX Traffic Manager detects applications with a combination of layer-7 deep packet inspection (DPI) and behavioural traffic analysis. All major protocols used for peer-to-peer file sharing (P2P), instant messaging (IM), media streaming, Internet telephony (VoIP), tunneling and online gaming are supported" (Ipoque, PRX Traffic Manager Solution, http://www.ipoque.com/userfiles/file/datasheet-prx10g.pdf).

5 Procera Networks, PacketLogic PL10000 Series, http://www.proceranetworks.com/images/documents-2011-02-24/PRE_PL10000_Q1_2011_2_23.pdf.

6 Arbor Networks, Arbor e100: Broadband Traffic Management, http://www.arbornetworks.com/arbor-e100-broadband-traffic-management.html

Davide Morisi – davidemorisi@gmail.com – www.davidemorisi.com

4.3. Chi la utilizza

Nessun sito ufficiale dei maggiori ISP italiani, americani, inglesi e canadesi fa riferimento all'uso della DPI. Recenti casi legali, tuttavia, hanno dimostrato l'uso di questa tecnologia da parte del maggior internet service provider inglese, la **BT** (European Commission, 2009), e di due fra i maggiori ISP americani, **Comcast** e **Cox** (Sandoval, 2008: 658, e Anderson, 2008).

Altri dati suggeriscono che la DPI è stata utilizzata o è attualmente in uso da parte degli operatori:

- inglesi: **T-mobile** (Rubenstein, 2010: 14), **VirginMedia** (Anderson, 2010a), **TalkTalk** (No DPI, 2008);
- canadesi: **Bell Wireline**, **Cogeco**, **Xplorenet** (Parsons, 2009: 24);
- spagnoli: **Yoigo** (Rubenstein, 2010: 14).

In Italia, un caso recente ha coinvolto la **Telecom Italia**, dopo l'annuncio da parte dell'azienda di introduzione di "meccanismi temporanei e non discriminatori di limitazione all'uso delle risorse di rete disponibili" (http://www.telecomitalia.it/assistenza/info-consumatori/news-187/novit%C3%A0-gestione-servizi-adsl). In particolare, su un blog della stessa Telecom Italia, viene dichiarato che Telecom Italia utilizza la tecnologia DPI, anche se "il DPI implementato da Telecom Italia non entra mai nel merito del 'payload applicativo' (per es. non viene presa in considerazione nessuna informazione sul contenuto del file scambiato)" (http://eraclito.telecomitaliahub.it/2011/02/quattro-risposte-tecniche/).

In generale, anche se non dichiarato sui siti ufficiali, il fatto che la maggior parte degli ISP dichiari esplicitamente di ridurre il traffico derivante dall'uso del peer-to-peer (P2P) lascia presupporre l'uso di qualche dispositivo di DPI, dal momento che altre forme di gestione del traffico non sarebbero in grado di discriminare i vari dati a un livello così profondo.

4.4. Benefici

In estrema sintesi, la tecnologia DPI permette di:

a) dare **priorità alle applicazioni sensibili al fattore tempo**, come il VOIP o lo streaming video;

b) **bloccare contenuti illegali**;

c) **contrastare applicazioni dannose** per la rete stessa o per gli utenti (come virus e malvare).

Alcuni autori aggiungono anche il potenziale benefico in campo militare o, in generale, di difesa delle reti da attacchi esterni (Gilder su Forbes, 2011).

4.5. Effetti negativi e potenziali rischi

L'uso della DPI si rivela tuttavia potenzialmente rischioso in relazione a diversi ambiti:

a) **potenziale tecnologico**: l'uso della DPI avviene in maniera totalmente "invisibile" e senza che l'utente si accorga di nulla (Cooper, 2010);

b) **riduzione della concorrenza nel mercato**: possibilità di creare "colli di bottiglia" concorrenziali (Ofcom, 2010: 18), dal momento che gli ISP si trovano in una posizione di vantaggio rispetto sia agli utenti finali, sia ai fornitori di contenuti;

Davide Morisi – davidemorisi@gmail.com – www.davidemorisi.com

c) **politiche discriminatorie di *pay for priority***: possibilità di offrire diverse velocità di connessione a seconda di contenuti specifici. Questo tipo di politica viene ampiamente criticato dalla FCC (2010: 43) in quanto può causare danni in termini di innovazione e può danneggiare gli utenti che utilizzano internet a fini non commerciali;

d) **riduzione del miglioramento delle reti a livello infrastrutturale**: la DPI può spingere gli ISP ad aumentare la velocità di navigazione non attraverso il miglioramento effettivo della capacità delle reti, ma discriminando l'uso di certe applicazioni (ad esempio rallentando in maniera estrema quelle applicazioni che utilizzano maggiormente la banda).

4.6. Rischi per la privacy

Infine, l'utilizzo della tecnologia DPI ha una serie di implicazioni negative per quanto riguarda la **privacy e la protezione dei dati personali**. Il fatto che la DPI è in grado di "leggere in profondità i pacchetti dati e assemblarli in una sintesi leggibile delle vostre email, le navigazioni in internet, le chiamate tramite VOIP e le password" (Anderson, 2007) solleva inevitabilmente grosse preoccupazioni. Questo punto, in particolare, è evidenziato dalla Commissione europea (European Commission, 2010b: 3), dall'autorità per le comunicazioni canadese (CRTC, 2009: par. 97) e dallo European Data Protection Supervisor (2010: 2).

Un chiaro esempio di questo uso illegittimo è l'applicazione della tecnologia **Phorm** (basata su una forma di DPI) che è stata utilizzata dalla BT nel 2006 e 2007 (European Commission, 2009), dalla Carphone Warehouse e da Virgin Media (Story, 2008) per raccogliere i dati degli utenti e rivenderli agli inserzionisti pubblicitari, in modo da recapitare messaggi pubblicitari estremamente mirati.

La DPI può dare inoltre adito a pratiche di **sorveglianza online**, come testimoniato dall'applicazione di questa tecnologia da parte di alcuni regimi non democratici (un esempio recente proviene dall'Iran: Rhoads e Chao, 2009).

In sintesi, con le parole del fondatore del Web, Tim Berners-Lee, "l'accesso di un ISP alle informazioni di un pacchetto internet che vada oltre l'informazione utilizzata per l'indirizzamento **è equivalente a intercettare un telefono o aprire un lettera sigillata**" (2009).

Quesito 5.

Quali sono i potenziali problemi concorrenziali derivanti dalla diffusione delle nuove forme di gestione del traffico? Le norme a tutela della trasparenza delle condizioni economiche e tecniche dei servizi offerti sono sufficienti a prevenire l'attuazione di comportamenti anticoncorrenziali nei mercati dei servizi dati? (…)

5. Oltre le norme per la trasparenza

In conclusione, in riferimento al quesito numero 5, è chiaro come l'utilizzo di tecniche come la Deep Packet Inspection sollevi una serie di problemi e preoccupazioni, non solo legati alla struttura del mercato, ma anche alla protezione dei dati personali.

Il nodo della questione è la potenzialità di questa tecnologia dal punto di vista degli ISP, sia a livello tecnologico (poiché può essere utilizzata in modo invisibile), sia, soprattutto, a livello di possibili maggiori guadagni. La DPI, infatti, permette agli ISP di adottare una serie di pratiche che si rivelano altamente redditizie (come la vendita di dati personali agli inserzionisti pubblicitari o il blocco di applicazioni concorrenti), ma che vanno ben al di là degli obiettivi ragionevoli di gestione del traffico già indicati dalla FCC.

Davide Morisi – davidemorisi@gmail.com – www.davidemorisi.com

È evidente, quindi, come si apra lo spazio per un necessario intervento regolamentativo. In questo senso, le norme per la trasparenza sono fondamentali, ma andrebbero potenziate, obbligando perlomeno gli ISP a dichiarare l'uso della DPI o di un'altra eventuale tecnologia di gestione del traffico che permette la raccolta di dati personali. Forme estreme di intervento potrebbero riguardare la totale messa al bando di tecnologie che consentono di per sé il raggiungimento di obiettivi "non ragionevoli".

Infine, per quanto riguarda il dibattito generale sulla neutralità della rete, l'applicazione di queste tecnologie avanzate di gestione del traffico deve indurre a un cambiamento di paradigma. Sulla scia di quanto già indicato da Wu, si tratta infatti di pensare a un "nuovo principio di neutralità della rete", secondo cui l'introduzione di forme di gestione del traffico viene intesa come necessaria per garantire *un'effettiva neutralità* di trattamento nei confronti di tutte le molteplici applicazioni che si sono evolute a pari passo con internet. Nello scenario tecnologico attuale, infatti, diviene indispensabile attribuire la giusta priorità a quelle applicazioni la cui stessa esistenza dipenda dal fattore tempo e dalla totale simultaneità fra invio e ricezione dei dati.

Il passaggio successivo consiste quindi nel definire quali forme di gestione del traffico possono essere definite accettabili e, in particolare, delimitare chiaramente le possibilità di azione degli internet service provider nei confronti della privacy degli utenti. Proprio il terreno della protezione dei dati personali, infatti, è destinato a diventare sempre più materia di scontro e dovrà perciò entrare con forza in un dibattito sulla neutralità della rete che finora è stato ampiamente dominato da un approccio largamente economico e di mercato (vedi al riguardo Ohm 2009: 1496).

Davide Morisi – davidemorisi@gmail.com – www.davidemorisi.com

6. Bibliografia

6.1. Consultazioni pubbliche sulla neutralità della rete

Agcom (2011a), Neutralità della rete: avvio di consultazione pubblica, Delibera n. 40/11/CONS, Gazzetta Ufficiale della Repubblica italiana n. 54.

Agcom (2011b), Consultazione pubblica sulla neutralità della rete, Allegato B alla delibera n. 40/11/CONS.

AGCOM (2011c), Garanzie dei consumatori e tutela della concorrenza con riferimento ai servizi VoIP e peer-to-peer su rete mobile, Allegato B alla delibera n. 39/11/CONS.

CRTC, (2009), Review of the Internet traffic management practices of Internet service providers, File number: 8646-C12-200815400, 21 October.

European Commission (2010c), Digital Agenda: consultation reveals near consensus on importance of preserving open internet, [press release], 9 November.

European Commission(2010b), Report on the public consultation on 'The open internet and net neutrality in Europe', 9 November.

European Commission, (2010a), Public consultation on the open internet and net neutrality in Europe, 30 June.

FCC (2010), Report & Order on Net Neutrality, n. 10-201, 23 December.

OFCOM (2010), Traffic Management and 'Net Neutrality' – A discussion document, 24 June.

6.2. Altre referenze

Anderson, N. (2007), Deep packet inspection meets Net neutrality, CALEA, *Ars Technica*, [online] 25 July.

Anderson, N. (2010b), Deep packet inspection soon to be $1.5 billion business, *Ars Technica*, [online] 16 June.

BEREC (2010), Response to the European Commission's Consultation on the Open Internet and Net Neutrality in Europe, 30 September.

Berners-Lee, T. (2009), No Snooping, *W3C*, [online] 9 March.

Cooper, A. (2010), The Singular Challenges of ISP Use of Deep Packet Inspection, *Deep Packet Inspection.ca*, [online].

European Commission (2009), Telecoms: Commission launches case against UK over privacy and personal data protection, [press release], 14 April.

European Data Protection Supervisor (2010), Comments on Net Neutrality and Traffic Management, 6 October.

Forbes, S. (2011), Steve Forbes Interview: Gilder On Tech Innovation, *Forbes*, [online] 14 February.

Mantellini, M. (2010), Quattro semplici risposte (tecniche), *Eraclito*, [online] 28 February. Disponibile su: http://eraclito.telecomitaliahub.it/2011/02/quattro-risposte-tecniche/

Parsons, C. (2009). Summary of January 13, 2009 CRTC Filings by Major ISPs in Response to Interrogatory PN 2008-19 with February 9, 2009 Updates, [online].

Paul Ohm (2009), The Rise and Fall of Invasive ISP Surveillance, *University of Illinois Law Review*, 5.

Rhoads, C. and Chao, L. (2009), Iran's Web Spying Aided By Western Technology, *Wall Street Journal*, 22 June.

Rubenstein, R. (2010), Deep Packet Inspection. Up Close, *Total Telecom Plus*, [online] April.

Story, L. (2008), A Company Promises the Deepest Data Mining Yet, *The New York Times*, 20 March.

Telecom Italia (2011, 15 February), Novità per la gestione dei Servizi ADSL. Disponibile su: http://www.telecomitalia.it/assistenza/info-consumatori/news-187/novit%C3%A0-gestione-servizi-adsl

Wu, T. (2003), Network Neutrality, Broadband Discrimination, *Journal on Telecommunications and High Technology Law*, 2