SAPIENZA
UNIVERSITÀ DI ROMA

FUB
Fondazione Ugo Bordoni
Ricerca e Innovazione

DDL - 2484 – Verifica tecnica della neutralità della rete e degli apparati

Antonio Sassano

Roma 28 Settembre, 2017

Regole Europee

- ***Regolamento 2015/2120 Parlamento Europeo e Consiglio***
- ***Regole del BEREC (31 Agosto 2016)***
  - ***No allo zero-rating e alla discriminazione del traffico***
  - ***Traffic management solo se «giustificato»*** *(verifica NRA)*
  - ***Servizi speciali consentiti*** *(«ben» definiti e motivati da QoS)* – ***5G possibile***
  - ***Misurazione ed enforcement affidati alla NRA***

Enforcement

178. In order to ensure compliance with the Regulation, and to promote the continued availability of non-discriminatory IAS at levels of quality that reflect advances in technology, NRAs could decide to:

- require an ISP to take measures to eliminate or remove the factor that is causing the degradation;
- set requirements for technical characteristics to address infringements of the Regulation, for example, to mandate the removal or revision of certain traffic management practices;
- impose minimum QoS requirements;
- impose other appropriate and necessary measures, for example, regarding the ISPs' obligation to ensure sufficient network capacity for the provision of high-quality non-discriminatory IAS (Recital 19);
- issue cease and desist orders in case of infringements, possibly combined with periodical (daily/weekly) penalties, in accordance with national law;
- impose cease orders for specific specialised services unless sufficient capacity is made available for IAS within a reasonable and effective timeframe set by the NRA, possibly combined with periodical (daily/weekly) penalties, in accordance with national law;
- impose fines for infringements, in accordance with national law.

DDL – 2484 vs. Berec: Gestione del Traffico

Art. 3.

(Limiti alla gestione del traffico)

1. Compatibilmente con gli orientamenti attuativi relativi all'articolo 3, paragrafo 5, del regolamento (UE) 2015/2120 del Parlamento europeo e del Consiglio, del 25 novembre 2015, ai fornitori di reti o di servizi di comunicazione elettronica non è consentito ostacolare l'accesso ad applicazioni e servizi *internet*, ovvero rallentarlo rispetto alla velocità alla quale sarebbe fornito a un utente nella stessa area avente la medesima capacità di banda e con accesso illimitato alla rete *internet*, fatti salvi i casi in cui le misure che ostacolano o rallentano l'accesso siano necessarie, comunque per brevi periodi, per una delle seguenti ragioni:

a) prevenire o mitigare gli effetti della congestione del traffico nella rete *internet*, a condizione che tipologie differenti di traffico siano trattate con le medesime modalità;

b) preservare l'integrità e la sicurezza della rete *internet* nonché del servizio del fornitore di reti o di servizi di comunicazione elettronica interessato o del terminale dell'utente finale;

c) limitare la trasmissione di comunicazioni non richieste a un utente finale, previo consenso dello stesso utente;

d) dare attuazione a specifici, cogenti e inderogabili provvedimenti legislativi o giurisdizionali.

"Objectively different technical QoS requirements of traffic categories"

62. In assessing whether a traffic management measure is reasonable, NRAs should assess the justification put forward by the ISP. In order to be considered to be reasonable, a traffic management measure has to be based on objectively different technical QoS requirements of specific categories of traffic. Examples for technical QoS requirements are latency, jitter, packet loss, and bandwidth.

63. Traffic categories should typically be defined based on QoS requirements, whereby a traffic category will contain a flow of packets from applications with similar requirements. Therefore, if ISPs implement different technical QoS requirements of specific categories of traffic, this should be done objectively by basing them on the sensitivity to QoS requirements of the applications (e.g. latency, jitter, packet loss, and bandwidth). For example, such a category may consist of real-time applications requiring a short time delay between sender and receiver.[18]

64. Based on this, reasonable traffic management may be applied to differentiate between objectively different *"categories of traffic"*, for example by reference to an application layer protocol or generic application types (such as file sharing, VoIP or instant messaging), only in so far as:

- the application layer protocol or generic application types require objectively different technical QoS;
- applications with equivalent QoS requirements are handled agnostically in the same traffic category; and
- justifications are specific to the objectives that are pursued by implementing traffic management measures based on different categories of traffic.

- *Miglior definizione di «**QoS requirements**» in termini di latency, jitter, packet loss e banda.*
- ***Differenziazione oggettiva** tra le diverse categorie di traffico (compito AGCOM)*

DDL – 2484 vs. Berec : *Prioritizzazione*

Articolo 3(2-3)

- *Prioritizzazione nell'**accesso***
- *«Best Effort garantito»*

2. In coerenza con gli orientamenti attuativi relativi all'articolo 3, paragrafo 5, del regolamento (UE) 2015/2120, i fornitori di reti o di servizi di comunicazione elettronica possono commercializzare servizi a valore aggiunto di prioritarizzazione di classi di traffico nel proprio segmento di rete di accesso per soddisfare specifiche esigenze della clientela d'affari e residenziale. L'adesione dell'utente deve essere liberamente espressa, anche per via telematica, e costituire oggetto di uno specifico e separato accordo tariffario e contrattuale. L'accesso *best effort* alla rete *internet* deve in ogni caso far parte dell'offerta degli operatori ed è pubblicizzato, con la stessa evidenza, nelle medesime offerte commerciali di cui al primo periodo, delle quali deve costituire la tariffa base.

3. Ai fornitori di servizi di accesso alla rete *internet* non è consentito fissare il prezzo per tali servizi in funzione dei servizi o delle applicazioni che sono offerti o utilizzati tramite l'accesso fornito alla rete *internet*.

?

50. As Article 3(3) concerns the equal treatment of all traffic *"when providing internet access service"*, the scope of this paragraph excludes IP interconnection practices.

99. Beyond the delivery of applications through the IAS, there can be demand for services that need to be carried at a specific level of quality that cannot be assured by the standard best effort delivery.

100. Such services can be offered by providers of electronic communications to the public (PECPs), including providers of internet access services (ISPs), and providers of content, applications and services (CAPs).

101. These providers are free to offer services referred to in Article 3(5), which BEREC refers to as specialised services[26], only when various requirements are met. Article 3(5) provides the safeguards for the provisioning of specialised services which are characterised by the following features in Article 3 (5) first subparagraph:

- they are services other than IAS services;
- they are optimised for specific content, applications or services, or a combination thereof;
- the optimisation is objectively necessary in order to meet requirements for a specific level of quality.

102. Their provision is subject to a number of conditions in Article 3(5) second subparagraph, namely that:

- the network capacity is sufficient to provide the specialised service in addition to any IAS provided;
- specialised services are not usable or offered as a replacement for IAS;
- specialised services are not to the detriment of the availability or general quality of the IAS for end-users.

103. According to Recital 16, the service shall not be used to circumvent the provisions regarding traffic management measures applicable to IAS.

104. All these safeguards aim to ensure the continued availability and general quality of best effort IAS.

DDL – 2484 vs. Berec : *Sicurezza della Rete*

Articolo 3(4) Minacce ad integrità e sicurezza della Rete

4. Se un danno all'integrità o alla sicurezza della rete *internet* ovvero al servizio del fornitore di reti o di servizi di comunicazione elettronica o ai terminali di utenti finali, di cui al comma 1, lettera *b)*, è causato dal traffico proveniente dal terminale di un altro utente finale dei servizi dell'operatore,

tivo e grave pericolo di danno all'integrità o alla sicurezza della rete *internet* ovvero al servizio del fornitore o di serio danno ai terminali di utenti finali, di cui al comma 1, lettera *b)*, il fornitore di reti o di servizi di comunicazione elettronica segnala tale circostanza, entro sei ore dalla scoperta, all'autorità giudiziaria, al *Computer Emergency Response Team* (CERT) nazionale, istituito presso il Ministero dello sviluppo economico ai sensi del comma 4 dell'articolo 16-*bis* del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259, e all'Autorità per le garanzie nelle comunicazioni, fornendo i dati tecnici strettamente necessari per prevenire il fatto dannoso nel rispetto delle norme a tutela della riservatezza dei dati personali.

83. Typical attacks and threats that will trigger integrity and security measures include:
    - flooding network components or terminal equipment with traffic to destabilise them (e.g. Denial of Service attack);
    - spoofing IP addresses in order to mimic network devices or allow for unauthorised communication;
    - hacking attacks against network components or terminal equipment;
    - distribution of malicious software, viruses etc.

84. Conducting traffic management measures in order to preserve integrity and security of the network could basically consist of restricting connectivity or blocking of traffic to and from specific endpoints. Typical examples of such traffic management measures include:
    - blocking of IP addresses, or ranges of them, because they are well-known sources of attacks;
    - blocking of IP addresses from which an actual attack is originating;
    - blocking of IP addresses/IAS showing suspicious behaviour (e.g. unauthorised communication with network components, address spoofing);

86. Besides monitoring the integrity and security of the network, possible security threats may also be identified on the basis of reports/complaints from end-users or blocking lists from recognised security organisations.

87. This exception could be used as a basis for circumvention of the Regulation because security is a broad concept. NRAs should therefore carefully assess whether the requirements of this exception are met and to request that ISPs provide adequate justifications[23] when necessary.

- ***Miglior definizione*** *di minaccia alla sicurezza ed integrità della rete (per evitare aggiramenti della norma da parte dell'ISP).*
- ***Valutazione oggettiva*** *«.. NRA should carefully assess..» del verificarsi delle condizioni*

DDL – 2484 e Device Neutrality

Articolo 4 - Device Neutrality

1. Gli utenti hanno il diritto di reperire in linea, in formato idoneo alla piattaforma tecnologica desiderata, e di utilizzare a condizioni eque e non discriminatorie *software*, proprietario o a sorgente aperta, contenuti e servizi leciti di loro scelta. Gli utenti hanno il diritto di disinstallare *software* e di rimuovere contenuti che non siano di loro interesse dai propri dispositivi, salvo

.. salvo

che tali *software* siano previsti come obbligatori da norme imperative o siano essenziali per l'operatività o per la sicurezza del dispositivo, delle reti pubbliche di comunicazioni alle quali si connette o dei dati gestiti dal dispositivo. È comunque vietata ogni disinstallazione effettuata al solo fine di consentire al dispositivo di funzionare in violazione di norme imperative.

«salvo che tali software … siano essenziali per l'operatività o per la sicurezza del dispositivo, delle reti pubbliche alle quali si connette o dei dati gestiti dal dispositivo»

- ***Giusto come principio generale*** *… e tuttavia* ***debole****.*
- ***Pensato per le App?*** *.. Ma allora perché solo* ***«disinstallare»*** *?*
- *Dire* ***«a priori»*** *se un* ***«software»*** *è* ***«essenziale»*** *è* ***molto difficile.***
- *La minaccia all'****Iphone*** ***o ai sistemi chiusi è solo teorica*** *..*
- *Apple potrà sempre* ***appellarsi alla essenzialità di ogni riga del suo software***
- ***Diritto alla garanzia?*** ***.. Molto lavoro per gli avvocati …***

DDL – 2484 - Conclusioni

- ***Qualche modifica al DDL 2484 è necessaria***
  - ***Art. 3:*** *superato dalle* ***Regole del Berec****,* ***andrebbe eliminato****.*
  - ***Art. 4:*** *giusto in principio ma* ***regole difficili da verificare*** *e dunque aggirabili e generatrici di contenzioso. Non saprei come ridefinirle.*

- ***Concentrarsi su Applicazione Regolamento UE e Regole Berec***

  - ***A che punto siamo con l'implementazione?***
    - ***AGCOM:*** ***Attività ancora allo stato iniziale***
    - ***CERT NAZIONALE:*** ***risorse insufficienti;***
    - ***Necessario impegno forte delle istituzioni*** ***(Parlamento e Governo) per:***

      - ✓ ***Attivare il monitoraggio*** ***del funzionamento della rete***
      - ✓ ***Definire e utilizzare metriche*** ***semplici da verificare***
      - ✓ ***Rafforzare i presidi di monitoraggio e verifica in termini di mezzi e personale***