Body of European Regulators
for Electronic Communications
BEREC

BoR (17) 241

BEREC Report on tools and methods used to identify commercial and technical practices for the implementation of article 3 of Regulation 2015/2120

7 December 2017

Contents

I. Introduction

In 2016 BEREC published Net Neutrality guidelines as mandated by the Regulation 2015/2120. This regulation also prescribes that NRAs shall *“closely monitor and ensure compliance” with the Regulation, and that NRAs shall “publish reports on an annual basis regarding their monitoring and findings”*.

One of the ways in which NRAs might identify contractual, commercial and technical practices introduced by ISPs at national level and assess their compliance with the provisions of Article 3 of the Regulation 2015/2120 is through the use of detection tools and methods, in particular three kinds: network diagnostic tests, processing of end-user reporting / complaints and regulatory surveys.

BEREC therefore reports on and analyses existing tools and suggests best practices. It will include a Technical and Commercial Practices Investigation (TCPI) template, similar to the one used in the BEREC/European Commission 2012 Traffic Management Investigation, for NRAs to use voluntarily as part of their future monitoring activities; the TCPI template can be valuable for preparation of the national implementation reports, in order to have a common scope of information.

This report was scheduled in the BEREC work programme of 2017 as the third workstream of the NN expert working group, entitled “Net neutrality supervision tools and methods”. In practice, this workstream also strongly benefits from inputs that stem from the two other workstreams of 2017, namely “Implementation of Regulation 2015/2120 and Guidelines on net neutrality” (workstream 1) and “Regulatory assessment of QoS in the context of net neutrality” (workstream 2).

Workstream 1 enables BEREC to review the best practices of NRAs when considering implementation of net neutrality regulation, including most of the supervision practices studied in this report. Workstream 2 has given insights into technical measurement tools that cannot only measure the quality of service of internet access service, but also the quality of service of specific applications within the internet access service, leading thereby to the detection of traffic management measures and potential infringements of net neutrality regulation.

Furthermore, the insights of workstream 2 were discussed during a dialogue with stakeholders in March 2017, so that experts from different industry sectors were able to comment on BEREC specification of tools and measurement methods. A specific attention was given to the detection of net neutrality infringements through distributed tools, which is detailed further on in this report.

II. Tools and methods allowing to identify commercial and technical practices

A. Key findings of Analysys Mason's study

BEREC commissioned Analysys Mason to study the approach taken by national regulatory authorities (NRAs) in selected non-European benchmark countries to address net neutrality issues. The benchmark countries were Chile, India and the USA. The study aimed to contribute to an informed public debate and constitute a valuable source of information for European NRAs and BEREC while they are implementing EU regulation 2015/2120.

The study also aimed to help BEREC and European NRAs to define their options for addressing net neutrality issues and identify the requirements and challenges they may face in the future. It should be noted that the study does not intend to include comparisons between the benchmark countries and the European regulatory framework. Although none of the benchmark countries has tools and techniques which have been specifically designed for monitoring non-net-neutral practices, the case studies illustrate interesting principles or monitoring approaches which may be of use to European NRAs as they develop their approach for addressing net neutrality.

According to the outcomes of the study, Quality of service (QoS) clearly has an impact on net neutrality, but the two concepts are quite distinct. Regulators in some markets are actively monitoring QoS, but have chosen to rely on a range of different methods to monitor net neutrality, such as qualitative reporting of traffic management practices by the ISPs, the 'seeding' of third-party initiatives, and having an established complaint system.

The important role of the complaint systems in the USA and Chile means that enforcement in these two countries has a primarily ex-post character. In Chile, tolerance of traffic management is checked against competition principles. In the USA, the FCC relies on telecoms law that was designed prior to the Internet era, to ensure reasonableness of prices, prohibit discrimination, respond to complaints, and impose penalties.

The report also concluded that third-party organisations can provide useful complements to the NRAs, in terms of expertise and capacity building in measurement systems suitable for the detection of certain types of net neutrality violations. Examples include the University of Chile and the Broadband Internet Technical Advisory Group (BITAG) in the USA.

Regulators are considering non – net neutrality practices across both fixed and mobile networks. In the case of mobile networks, crowdsourced smartphone app-based approaches for gathering measurements are being used in both Chile and the USA.

Many different tools are available to detect practices which may violate net neutrality (either ex-ante or ex-post), but it is unlikely that any single tool can provide a comprehensive solution. Incidents such as the Comcast/BitTorrent episode in the USA demonstrate that regulators will have difficulty anticipating every possible form of net neutrality abuse in advance. In the EU/EEA, NRAs are obliged to actively monitor non-net-neutral practices themselves. The technical requirements of doing so need to be carefully thought through and specific multiple tools or methods are likely to be required. This may imply the need, not for a single tool, but for a toolkit that can grow over time as new risks are identified and as new forms of abuse are encountered.

B. Key findings of BEREC internal factual report

This section includes a list of methods and tools that can be used to identify violations of the regulation. The list was compiled using the NRAs' answers to the "BEREC Internal Questionnaire on National Implementation of the Regulation (EU) 2015/2120" which was sent out by BEREC to compile the "BEREC Report on the implementation of Regulation 2015/2120 and related BEREC guidelines, including possible recommendations". BEREC received 29 answers on the questionnaire. Although the questionnaire covers all articles of the regulation, for this report only the relevant questions were considered.

The methods/tools used by the NRAs can be distinguished between tools that are monitoring practices under art. 3 and tools that are monitoring practices under art. 4 only. The focus of this report lies on the implementation of art. 3. Nevertheless, the following part incorporates tools to identify violations of art. 4 as well. In many cases one tool is used to detect violations of both articles of the regulation. The answers are summarised below.

Market survey without requesting information from ISPs

Market surveys without requesting information from ISPs were used by many NRAs for gathering information on several issues. This category of supervision tools includes – but is not limited to – checking ISPs' information on their web pages and the review of applicable terms and conditions (T&Cs) (see also relative section III.D).

Market surveys were also used to:

- monitor the commercial and technical conditions related to the provision of Internet Access Services (IAS),
- monitor traffic management practices by ISPs,
- monitor specialized services (SpS),
- monitor and enforce ISPs' compliance with their transparency obligations set out in art. 4 of the Regulation, and
- measure the availability of high quality IAS.

Information requests from ISPs

Information requests from ISPs cover all kinds of requests, e.g. questionnaires and the examination of the T&Cs (see also relative section III.D), under which ISPs provide Internet access services. These requests can be formal or informal.

This method was used to:

- monitor the commercial and technical conditions related to the provision of IAS
- monitor traffic management practices by ISPs
- monitor specialized services
- monitor and enforce ISPs' compliance with their transparency obligations set out in art. 4 of the Regulation
- measure the availability of high quality IAS.

Analysis of complaints and end-user reporting

End-user complaints and end-user reporting are important tools in many countries (see also relative section III.C). Most NRAs stated to monitor end-user complaints (22 member states). Usually, the complaints were related to discrepancies between actual and contractual speed, as well as other QoS (Quality of Service) parameters.

In most countries, NRAs have already established procedures for addressing end-user complaints in case of non-conformance of the provided services with the contractual terms. In general, such procedures had already been in place before the Regulation 2015/2120 came into force, as providers of IAS are required to do so as part of the existing telecoms legislation (which is based on the Universal Service Directive). No additional/specific complaint procedures have therefore been introduced in the majority of countries.

Generally, different channels are offered by ISPs, thus facilitating the introduction of complaints by end-users. The most common channels are telephony, web forms, letters and customer service centers.

End-user complaints were used to:

- monitor the commercial and technical conditions related to the provision of IAS
- monitor traffic management practices by ISPs
- monitor specialized services
- monitor and enforce ISPs' compliance with their transparency obligations set out in art. 4 of the Regulation
- measure the availability of high quality IAS.

Technical network monitoring

Technical network monitoring was used by many NRAs to:

- monitor the commercial and technical conditions related to the provision of IAS
- monitor traffic management practices by ISPs
- monitor specialized services
- measure the availability of high quality IAS.

Meetings with ISPs and/or stakeholders

A lot of NRAs held meetings with ISPs and/or stakeholders before and while implementing the Regulation. A few NRAs explicitly stated that they used meetings with ISPs and/or stakeholders to:

- monitor the commercial and technical conditions related to the provision of IAS
- monitor traffic management practices by ISPs
- monitor and enforce ISPs' compliance with their transparency obligations set out in art. 4 of the Regulation.

Meetings with ISPs were also used to provide guidance or impose additional transparency or information requirements on ISPs following the enforcement of the Regulation.

IAS quality monitoring mechanism for consumers

15 NRAs have introduced such a monitoring mechanism during the reporting period or had already one in place before. All of the reported monitoring mechanisms measure the speed of

end-users individual IAS in fixed and/or mobile networks. The monitoring mechanisms also allow to measure QoS parameters (generally: latency, jitter, packet loss). Of these, four NRAs reported that their monitoring mechanism is certified according to the Regulation and the BEREC Guidelines (paragraph 161).

The member states currently not having a national measurement system have plans to introduce such a mechanism: Some NRAs are supporting and/or contributing to the BEREC project regarding the BEREC NN measurement tool (more information on this is provided in section III.B). Besides this pan-European project, some NRAs have ongoing projects to set up their own monitoring mechanism.

NRA (internal) cooperation

Some NRAs used interdepartmental cooperation and held inter-NRA discussions or participated in joint projects, e.g. EC pilot project regarding QoS crowdsourcing. In some member states there is cooperation with (other) national authorities or entities on this subject.

Publications

In order to implement the Regulation, some NRAs published information for consumers and stakeholders. Also, press releases related to the Regulation were issued. Some NRAs created or improved their web pages regarding net neutrality issues. Some NRAs also provided checklists and product information sheets ISPs can use to inform their customers about transparency requirements related to art. 4 of the Regulation.

Other tools

Other measures used to implement the Regulation were non-technical surveys and price and/or offer comparison mechanisms/tools. To monitor and enforce ISPs' compliance with their transparency obligations set out in art. 4, surveys by 3rd parties and the publication of statistical comparative values of ISPs' QoS results reached in past periods (to motivate compliance) were used. Some NRAs used mobile coverage maps and RF measurements to measure the availability of high quality IAS.

To enforce the Regulation, some NRAs prepared a national draft legislation, national guidelines or a secondary legislation on an enforcement policy also concerning transparency issues. Some of them combined the above approaches.

C. Feedback from the stakeholders dialogue

As a step in its 2017 work program, BEREC has met with stakeholders to gather views. Meetings were held on 14, 15 and 16 March with stakeholder organizations at the European level representing internet service providers (ISPs), equipment manufacturers, measurement system providers and specialists, content and application providers (CAPs) and end users / consumer organizations / civil society.

At these meetings, BEREC was seeking the views of stakeholders on four topics:

- Measurement methodology on individual applications.
- Measurement methodology on IAS as a whole.
- Practical considerations regarding measurement systems.
- Net neutrality supervision tools and methods.

Particularly, the last topic is focused on achieving inputs to this report. Thus, panellists were invited to present their views on the tools and methods that can be used by NRAs to identify, on the one hand, and assess, on the other hand, technical and commercial practices falling under art. 3 of Regulation 2015/2120.

In that regard, Internet Service Providers and equipment manufacturers express the existence of two main dimensions in relation to tools and methods of supervision. Firstly, the level of transparency implemented by the ISP should be in keeping with the Regulation. And secondly, a service degradation solely should trigger an investigation by the NRA (e.g. based on proven sustained complaints from users). In this context, ISPs and equipment manufacturers suggest that a standardized method/form be explored for end-users to be able to get information from ISPs in case they experience a QoS problem.

The stakeholder group, comprised by measurement system providers and specialists, put emphasis on using any available diagnostic tests, tools or platforms, since there is an extensive range of reliable and tested tools in the market. In that regard, they highlight the DPI debate, and recall that this methodology could be used in the scope of the Regulation for security and legitimate purposes.

Likewise, as ISPs and equipment manufactures express, measurement system providers and specialists attach a great deal of importance to providing transparent practices by ISPs and analysing content delivery networks (CDNs) and their relationships with ISPs, as CDNs are a way to provide a fast access to content.

Regarding the content and application providers (CAPs), they point out the need for publishing a list of ISPs with services and connections in line with the Regulation. Also, this group remarks the problem of privacy with supervision platforms or tools.

Finally, end-users, consumer organizations and civil society groups highlight the idea of using as many tools as possible in order to detect net neutrality infringements: complaints, questionnaires, surveys, systematic analysis of contracts. After this step, an NRA intervention may start if needed. This group also wants to highlight the benefits of partnerships among NRAs, civil society and content providers to create tools and platforms for the need of reporting any Regulation infringements.

D. List of tools and methods

A list of tools and techniques that can be used in order to identify commercial and technical practices is featured below:

- Regulatory surveys (including technical and commercial practices investigation or “TCPI”).
- Network diagnostic tests (utilising various measurement platforms & methods).
- Processing of end-user reporting and complaints.
- Assessment of contract T&Cs.
- Formal requirements and proceedings.
- Third party investigations (associations, consumer organisations, end-user reporting platforms, etc.).

The summary matrix below shows tools, methods and techniques that could be used for the evaluation of commercial and technical practices. An extended version can be found in Annex 2.

		Commercial Practices	**Technical Practices**
		(e.g. Zero Rating, IAS and Content bundling, Sales conditions, Prohibition of some practices like VPN or tethering…)	(e.g. Traffic differentiation, Capacity reservation/allocation, Prioritisation, Blocking or throttling…)
Tools, Methods & Techniques	Network diagnostic tests		
	End-user reports & complaints		
	Assessment of T&Cs		
	Regulatory Surveys (incl. TCPI)		
	Market surveys		
	Third Party investigations		
	Formal proceedings		
	Meetings with ISPs and/or Stakeholders		
	NRA cooperation		
	Publications		

III. Best practices for NRAs on tools and methods allowing to identify commercial and technical practices

A. Network diagnostic tests

BEREC has developed a regulatory assessment methodology in order to support National Regulatory Authorities (NRAs) with the implementation of the net neutrality provisions of the Regulation 2015/2120. It is intended to help NRAs in the monitoring and supervision of the net neutrality provisions of the Regulation based on various net neutrality measurement tools and a harmonised measurement methodology for quality of service indicators.

In this document, BEREC specifies the methodology for the measurement of IAS speed to enable NRAs to assess IAS performance compared to the contractual minimum, normally available and maximum speed values, as well as other QoS parameters.

Furthermore, the document gives recommendations on various tools for detecting traffic management practices that impact individual applications and suggests other indicators of performance closer to the user experience. It includes recommendations for detecting traffic management practices that affect the connectivity and ultimately a possibility to use and provide individual applications. The document describes also recommendations for detecting traffic management practices that affect the quality of individual applications, like the prioritisation and/or throttling of specific applications.

Additional information is given for developing and implementing crowdsourcing-based measurement setups. An overview on the most important factors that should be taken into account when assessing the measurement results is given and also guidance on collecting this information.

Finally, recommendations for the validation of the collected measurement results are provided and also some further guidance on how the speed measurement results should be assessed in comparison to the contractual speed values for end users. The topic of data aggregation for market level assessment purposes is discussed and guidance on monitoring the general IAS quality (IAS as a whole and effect of specialised services on IAS), as well as individual applications using IAS is provided.

Based on this guidance, NRAs can develop and implement measurement systems used for assessing quality aspects and investigating on various NN issues that might occur in actual networks used for the provision of Internet access services. BEREC will also use this methodology in its development of a NN measurement tool which can be used by NRAs on an optional basis.

B. Processing of end-user reporting and complaints

Given the different national legal dispositions, NRAs may or may not have powers to intervene in the field of consumer rights. European NRAs may therefore have different approaches when dealing with queries that emanate directly from end-users: NRAs may have developed different levels of consumer relationship service. This could also make a difference, so far as NRAs consider end-user queries as “simply” reporting (with no automatic legal consequence) or more concretely as a formal complaint (that would entail to a procedure).

Nevertheless, it can be of some advantage to NRAs if they have access to consumer feedback, even in cases where there is no concrete legal power to handle their complaints. In a field like net-neutrality, where the nature of the practices of ISPs or other stakeholders are diverse and challenging to detect with automated tools, end-user complaints are a valuable source of information. Some users are able to set up documented cases on problems they have witnessed (especially when the NRA can suggest reliable detection or measurement tools for the end-user), some will only hint at a problem they are presuming, but in any case this can be a matter for the NRA to investigate (with more effective tools or by directly questioning the ISP). Of course, net neutrality is not the only topic that is concerned by reporting or complaints: contractual issues and transparency on quality of IAS are, for example, very likely to raise a large number of queries.

Besides of the handling of the cases themselves, it makes sense for an NRA to organise the information gathering and metadata from the end-user queries. It can help produce statistics in general and also statistical evidence (the repetition of a complaint in large numbers could be a hint that the underlying problem is serious and not an epiphenomenon).

For such use, it is beneficial for an NRA to enable consumers to file their case on a reporting platform, on which they can post some kind of self-assessment (for example, by categorizing their complaint in a specific type of problem), making it easier for the NRA to review a large number of contributions.

This concept is not only usable by NRAs. Consumer rights' associations like EDRI and LQDN have developed for example a European-wide reporting platform specifically dedicated to net neutrality issues. It enables end-users to post a short description of the problem they witnessed and to file them in a specific category of problems in order to facilitate their review. In this case, the submitted cases are displayed publicly on the webpage of the initiative, in a sort of name and same approach that gives an incentive to ISP to be compliant with Regulation 2015/2120 in order to avoid image damage.

However, it might be complicated for NRAs to follow that same approach (e.g. create a nation-wide reporting platform), considering the potential legal issues with unverified consumer complaints. It is also of utmost importance that NRAs, if opting for a reporting platform, they consider the issue of data privacy when gathering end-user data for the handling of each case or the related statistics.

C. Assessment of terms and conditions

The assessment of T&Cs is more related to transparency obligations laid out in art. 4, but also practices falling under art. 3 could be detected by assessing public documents as well as tariff information from ISPs. T&Cs as well as tariff information also include information about practices falling under art. 3. By assessing this information, NRAs may detect violations of art. 3, e.g. sub-internet services restricting end-user rights set out in art. 3(1), e.g. exclusion of VOIP services, zero-rating practices (art. 3(2)), information about traffic management (art. 3(3)), etc.

A good method to check compliance is to nationally implement an assessment of T&Cs as well as tariffs and marketing information. As laid out in para. 21 of the guidelines "BEREC considers that the Regulation does not require an ex ante authorisation in relation to commercial practices (Article 3(2)), traffic management practices (Article 3(3)) and specialised services (Article 3(5)).” Yet, this information may be assessed ex post. Consequently, end-users have the possibility to make a formal complaint if the contractual terms are not met, so that NRAs can initiate further investigations.

The guidelines list several remedies in case the obligations under art. 4 are not met: “158. Remedies available to consumers as described in Article 4(1) (e) are defined in national law. Examples of possible remedies for a discrepancy are price reduction, early termination of the contract, damages, or rectification of the non-conformity of performance, or a combination thereof. NRAs should ensure that ISPs provide consumers with information specifying such remedies.”

D. Other tools and methods

On top of the above and as extra alternatives, NRAs might consider using other tools and methods such as:

- findings from formal proceedings or third party investigations,
- the ‘record and reply’ method, seeking to replicate end-users’ experience detecting traffic differentiation for arbitrary applications in the mobile environment (http://david.choffnes.com/pubs/Differentiation-IMC.pdf),
- other existing end-user reporting platforms, such as http://dd.meddle.mobi or
- other measurement visualization platforms, such as M-LAB (https://viz.measurementlab.net),
- on-line tools for monitoring and comparing various broadband packages & commercial offers, such as https://www.pricescope.gr/home, http://www.bestetarief.be, https://www.comreg.ie/price-comparison, or https://www.anacom.pt/tarifarios/PaginaInicial.do?channel=graphic
- offering a protected space for whistle-blowers to submit their experience, measurements, information on traffic management practices, etc. (e.g. https://www.business-keeper.com/en/systematic-compliance/bkms-system-en.html).

E. Other considerations

Regulatory surveys

On February 1, 2017 the BEREC NN EWG requested from all NRAs to provide: *“… short information on any detection tools and methods [your NRA] has or used recently regarding the Regulation 2015/2120... This could mean mainly three types: automated assessment tools (such as network diagnostic tests), end-user reporting platforms and periodic questionnaires. In case you have circulated or prepared a questionnaire aiming at identifying practices falling under Regulation 2015/2120, please provide us the template of this questionnaire”.*

21 NRAs responded, among which 14 submitted their questionnaire templates (key findings of their answers are listed in section II.B above). While compiling these templates, it became clear that each NRA had a different approach. Some NRAs focused on a singular subject with very detailed questions, while other NRAs adopted a more general approach with general questions on a broad number of subjects. There was very little synergy to be found

among these templates. To value each approach, all national templates were merged into a single BEREC template that covers most aspects of the regulation, including questions of considerable detail. The BEREC template should therefore be considered as a buffet, where each NRA may select – or even add – the elements they deem necessary to investigate before sending the questionnaire to their operators. The questionnaire template for voluntary investigation of technical and commercial practices on a national basis is attached to the report [Annex 2].

NRAs might also consider getting additional information from resources and organisations allocated to the implementation of NN legislation / regulation, such as:

- ISPs' complaints and reports on network performance issues of other carriers/ISPs
- Other institutions' reports & measurement platforms on Traffic Management (TM) practices (e.g. http://netalyzr.icsi.berkeley.edu or https://www.broadbandmapping.eu).
- BEREC database on TM cases with best practices/tools on network and IAS performance; could be stored and maintained, ready to be offered to experts that would like to run the same processes for their own arbitrary applications in their respective countries
- Reporting / monitoring via existing or new QoE KPIs on ISP's network and traffic management performance. The majority of European ISPs either are offering publicly available their own KPIs or they reporting to NRAs the requested QoE KPIs along with network performance KPIs.

Annex 1 – Commercial and technical practices covered by article 3 of the Regulation (EU) 2015/2120

Here below you may find a list of the commercial and technical practices and their sub-categories as these are used in the Technical and Commercial Practices Investigation (TCPI) template. This is a template that serves the purpose of assisting NRAs in their NN supervisory role and may be sent to ISPs either 'as is' or modified according to their national needs. Although the TCPI template was intended to accompany this report, it could not be embedded in the document due to its big size. Therefore, for the completion of this document it was deemed appropriate to list the aforementioned practices as shown below:

Commercial practices

- Zero-rating, IAS and content bundling, sponsored data;

  Zero-rating: Data from a certain application/content provider does not count towards the data cap of the tariff plan. There is not necessarily a commercial link between the ISP and application / content provider.

  i. Zero-rating within the data cap: all data is treated the same after reaching the data cap.
     1. Zero-rating of specific categories of applications, like Video streaming, Audio streaming, Social media, Messaging, VOIP, News content, etc.
     2. Zero-rating of individual applications.

  ii. Zero-rating beyond the data cap: technically unequal treatment of data, as the zero-rated services and applications are not blocked or throttled once the data cap is reached, while others are.

  iii. IAS and content bundling: The subscription fee to the content service is included in the monthly fee. If the data of the content service is zero-rated, then this practice should also be categorized under the zero-rating practice.
     1. Promotional offers, e.g. free Netflix or Spotify subscriptions (for a limited amount of time).
     2. Provision of IAS + zero-rating of a specific product.
     3. Provision of IAS + a specific product/application/category of applications with a specific additional cap.

- Prohibition of some practices, e.g. use of VPN, tethering.
- Other commercial practices: all services included in the offer in parallel to the internet access service (e.g. bundling of software such as Office, as well as complementary services like access to Wi-Fi hot spot network).

Technical practices

- Capacity reservation/allocation: e.g for ISP-preferred or ISP-owned content or applications or an agreement with a content /application provider to guarantee a better quality of service for its traffic.

- Offers with guaranteed throughput rate, e.g. traffic management policies that enable a stable throughput rate for specific content or applications.
- Prioritisation of some users, or of some service, protocol, content, or application:
    i. Prioritisation of business users over private users.
    ii. Prioritisation of specific applications, e.g. IPTV, VPN, VoLTE, signalling/network management traffic etc.
    iii. Prioritisation of tariffs, e.g. some tariffs are prioritised according to their specific characteristics e.g. speed.
    iv. Prioritisation of certain providers, e.g. commercial providers for video streaming vs. non-commercial providers (e.g. T-Mobile US's "Binge on").
- Class-based traffic differentiation.
- Choice of terminal equipment: e.g. permitting network connection only via pre-specified white-listed CPE / routers.
- Limitations in wholesale access: e.g. if – as a bitstream buyer – you are unable to perform policies like multicasting on those (fixed) access types, or you are limiting the bandwidth for customers that are on roaming (for mobile).
- Modification of content or traffic, e.g. image or video compression by stripping out advertising.
- Blocking or throttling of some users, of some specific content or application types (e.g. VoIP, streaming, peer-to-peer file sharing, newsgroups) or some port or protocol (e.g. SMTP), or prohibiting some practices (e.g. use of VPN, tethering):
    i. Blocking of specific user categories.
    ii. Blocking of specific content or application types (e.g. VoIP, streaming, peer-to-peer file sharing, newsgroups, Instant Messaging).
    iii. Blocking of specific content / application providers.
    iv. Blocking of specific web sites, domain names or networks, e.g. blocking or throttling of certain IP addresses for incoming / outgoing traffic in the network or in the customer terminal equipment.
    v. Blocking of some port or protocol, e.g. blocking or throttling of certain TCP / UDP ports and / or certain protocols for incoming / outgoing traffic in the network or in the customer terminal equipment.
- Assurance of IAS availability and quality (e.g. availability of sufficient capacity for IAS in case a specialized service is offered).

Annex 2 – TCPI template

In attachment to this report.