OTT REGULATION A WAY OF COMBATING CYBERCRIMES

Veronica Mocanu[1]

DOI: 10.24989/ocg.v331.33

Abstract
In the past decade we have witnessed a rapid expansion of the Internet gadgets, Internet services and internet applications. This revolutionary communication network has significantly changed the way people live, communicate, and conduct business. However, from legal perspective all of these new challenges remain under covered, things that frequently could generate harm, abuses and cybercrimes. Therefore, by this research, it is proposed to discuss the main risks, which are generated by using of uncontrolled OTT and present perspectives of regulations. The article includes topics such as description of OTT regulations practices used for the moment, problems generated by chaotic regulations of OTT, perspective that we have to take, need for licensing and certification of new internet applications and services, setting of quality standards, and proposes for involvement in development.

1. Introduction

In the last 30 years, contemporary societies are involved in a continuous activity of developing and promoting the use of information technologies. There are intensively promoted actions of digitization and automation of human activity in such a way that human existence to be maximized. As a result, we find that efforts are not in vain, and the living conditions really have changed. If, 30 years ago, using the smartphones or remote control devices seemed utopian, today these are an indispensable part of human activity.

Moreover, not only living conditions, but also the forms of perception of reality and business development are changing. Today if you need a product you no longer have to go to the store, the product can be purchased online; if you prepare a bachelor thesis and you want to get informed, the internet is the most used way of documentation, here you can find last-minute news as well as information dating back to the previous centuries; if you want to go for vacation but you do not know which destination to choose, the internet gives you the description of the route, the hotel tour, pictures in online mode and even the real impressions of the tourists.

Through its existence, the Internet is changing the concepts, ways of existence, and the practices established for centuries.

Under the conditions of a digitalized life, digital information and communication have turned into indisputable values of contemporary human activity. Thus, through the possibilities, platforms and fields of activity available online, the Internet has been resized and it should no longer be interpreted only as a connection tool, it is to be regarded as a new medium of activity, the existence of which is determined by the technological conditions, human will, but also the legal framework.

[1] State University of Moldova, Law Faculty, Department of Public Law, Chisinau (Moldova), http://usm.md/

The on-line activity is not a virtual activity anymore, online activity has been significantly resized over the last few years, so that online activity is a real activity that produces real effects.

Thus, by this article, contrary to the replies that promote the idea of an unregulated Internet, we call for the regulation of the online domain, indicating that it is absolutely necessary, or only by regulation can be ensured a free, fair and equal environment for all subjects involved in use of the internet. We draw attention, however, that new regulations are to be developed only for new realities, and in other cases, the generally accepted rules can be applied by analogy.

As indicated above, the on-line domain is a multidimensional domain involving the activity of different actors in different areas. By this article, however, we propose to focus on researching the field of OTT, as a contemporary challenge of the information society today.

2. What are OTTs?

The concept of Over-The-Top (OTT) services has appeared in the audiovisual sector in the 2010s' to refer to the new market that was emerging alongside the traditional markets of television (hertzian, satellite and cable television) that included new forms of delivering audio and other media content over the Internet. Today, this concept commonly refers to the provision of content and applications, including communications services over the Internet (e.g. voice services, hosting services, email services instant messaging, web-based content (news sites, social media, etc.), search engines, and video and multimedia content, etc). Usual examples of such services are WhatsApp for text messaging, Skype for video chat and voice call services, YouTube for video content sharing, Netflix and HBO for video streaming services, Spotify and Deezer for music streaming services, etc. [7].

Even though we already have at worldwide level different regulatory practices, at European level, we do not have yet an official position regard official concept, classification and regulation of the new OTT services so far, but generally, opinions are divided into three camps. The representatives of telecommunications companies, being affected by the appearance of new services, put forward arguments for awarding the OTT to the category of electronic communications services and applying for them the same rules as for electronic communications providers. Technicians and developers largely award the OTT to the information society services category, indicating that these services can be applied by analogy to the E-Commerce Directive. More and more are those who advocate the idea of appearance of a distinct form of services to which specific rules are to be applied, and OTTs are to be considered as distinct forms of communication.

The term of OTT came about as a result of more traditional telecom services coming under competition from content and service providers offering similar solutions using web services methods [6].

Wikipedia explains that "… over-the-top content (OTT) refers to delivery of audio, video, and other media over the Internet without the involvement of a [network] operator in the control or distribution of the content. The Internet provider may be aware of the contents of the Internet Protocol packets but is not responsible for, nor able to control, the viewing abilities, copyrights, and/or other redistribution of the content. This model contrasts with the purchasing or rental of video or audio content from an Internet service provider (ISP), such as pay television video on demand or an IPTV video service ..." [12].

Being aware of legislative gap, preparing a study regard OTT players, European Parliament mentioned that it makes clear that an OTT service is not a transmission network, but is instead a service that runs over an Internet network; moreover, the OTT service provider is typically distinct from the operator of the underlying network. From European Parliament's perspective an over-the-top (OTT) service is an online service that can be regarded as potentially substituting for traditional telecommunications and audiovisual services such as voice telephony, SMS and television [13].

In order to advance some clarifications for the moment, designing in January 2016 a report regard OTT services, the Body of European Regulators of Electronic Communications ("BEREC") defines OTT as "content, a service or an application that is provided to the end user over the open internet" and introduce notion of CAPs in sense of presenting the new category of internet players - content and applications providers [2]. Including in the definition that what is provided can be either content, a service or an application, means that anything provided over the open Internet is an OTT service. This provision generally occurs without involvement of the IAP in the control or distribution of the service. Because the service is provided over the Internet this definition implies that OTT refers to content that usually arrives from a third party (OTT provider), not being provided by the IAP to which the end user is connected. However, it is also possible the IAP offers its own OTT services or partners with OTT providers [2].

BEREC emphasizes that the definition of OTT does not have a legal status: OTT is not a term that has a meaning in the ECN/S Framework. OTT services do however have relevance in debate on the new ECN/S Framework.

Taking in consideration the above mentioned definitions, we will retain that for the moment, OTT refer in general to Internet-based content, applications and services that ride "over the top" of networks and are accessed by end users through a broadband Internet connection without the direct involvement of a network operator or Internet Service Provider.

However, in sense of preventing any misunderstanding, we find that OTT providers point that frequently, over-the-top term is wrongly used in the telecom world to describe any unmanaged service delivered over IP (online services). Opposite to the BEREC position, they promote to use "over the top" notion just to describe any content, services, or applications provided over an infrastructure that is not under the administrative control of the content or service provider. Thus, if an operator offers an IP service (say IPTV), and that service is delivered over the operator's infrastructure (whether mobile, fixed, or otherwise), it should not considered as OTT. However, if that same operator, after building a content/service model, extends the service to any IP end point on another operator's network, then it becomes OTT. Whether the operator decides to use QoS for the service is irrelevant in the definition of OTT. In other words, OTT providers promote the idea that an operator offering a service to its own subscribers could not be considered as an OTT player; rather if quality and bandwidth will be enforced, from OTT provider's opinion, the mentioned service will be considered just as a managed ECS[2], and if not, it will be qualified as an unmanaged ECS service (online services). Only if it is extended beyond the boundaries of that telecommunication's infrastructure is will be correctly referred to an OTT service or player [6].

[2] Providing managed ECS refers to providers which offering the service has control over the fixed or mobile access network used for its distribution. The provider is able to use this control to dimension the network, and in many cases to reserve network capacity to guarantee the quality of the service. Thus, managed services are strongly linked to the underlying network. Examples of such managed services are fixed and mobile telephony and the IPTV service offered by many network operators.

Personally, I accept the phenomenon of new internet realities linked to Internet-based content, applications and services provided, but I not agree with use of notion of OTT, and necessity of making differences between Internet-based content, applications and services provided by IP and Internet-based content, applications and services provided by third party. Analyzing the interpretation provided, seems that OTT term has been artificially introduced as a way to escape from the current legal framework, prevent assimilation with classic electronic communication providers and avoid the assumption of obligations.

I agree that Internet-based content, applications and services represent new realities and differ by classic electronic communication, but the accents has to be pointed not just on forms of delivery, and statue of the players, we also have to take in account the type of information administered by CAPs, risks involved in context of administration, users rights.

Revising the above mentioned, we had identify tree types of service providers which deal with similar business, but pretend to different levels of regulation, so we identified managed *electronic communication services providers*- the provider offering the service, has control over the fixed or mobile access network used for its distribution. The provider is able to use this control to dimension the network, and in many cases to reserve network capacity to guarantee the quality of the service. Thus, managed services are strongly linked to the underlying network. Examples of such managed services are fixed and mobile telephony and the IPTV service offered by many network operators; *online services providers* - providers who rely on the public Internet for at least parts of their distribution. The provider has little or no control over a part of the distribution network in particular the access networks. Well-known examples of online services are Skype and YouTube; and *OTT providers* - internet-based content, applications and services providers that ride "over the top" of networks and are accessed by end users through a broadband Internet connection without the direct involvement of a network operator or Internet Service Provider.

Taking into consideration the above mentioned, it is clear that the possibilities of ensuring the quality of services are different and that the operator has obligations prescribed by law to ensure the quality of the offered services, obligations to maintain confidentiality, neutrality and also interoperability, but to OTT providers are not prescribed for the time being such obligations, they specifying that to them can not even be prescribed such obligations because they have practically no technical possibilities.

The issue that appears is related to the content, and applications that allow entering not administered content. Thus, a question arises, would it be correct to distinguish the subjects involved in the online activity only after the way of operating the services, I refer in this respect to services / content / applications provided by the operator through his own network and services / content / applications over-the-top, that means through a foreign network? Or would it be appropriate, however, to differentiate the subjects also depending on the type of information being administered, the rights possible to be exercised, the risks involved?

In response to this question, we believe that in order to prevent confusions, the online subjects should be differentiated not only depending on how the content / applications / services are provided but also on the type of performed online activity. As a result, we could distinguish *content providers, application providers, service providers, internet providers,* etc., establishing separate obligations and rights for each category, in the same time pointing to the need to cumulate all rights and obligations derived from the subject`s status (player). Thus, if the operator is both an internet provider and an application provider, he shall assume both categories of rights and obligations.

We believe that by such an interpretation could be eliminated the inequality raised at the moment by internet operators, who are investing in infrastructure but whose services are declining. Similarly, this form of regulation would bring clarity about the legal status of each type of subject involved in online activity, stimulating growth and competitiveness.

3. Do Internet-based content, applications and services have to be regulated or not?

Regulation of internet is another complicate issue, and here we also have different opinions, tech field tray to argue that internet has to remain free, and there is no place for government rules, in opposite states try to demonstrate that unregulated Internet-based content, applications and services could present a danger. On European level, regulating authorities confirm the need for regulation and states that the existing regulatory framework does not apply to OTT per whole.

By, this article we will take the part of state, and will plead for regulation of Internet-based content, applications and services.

The lack of regulation leaves room for interpretation and maneuver, but at the same time it can transform the internet into a black hole that can generate the construction of a wrong world, built contrary to moral norms, common good and social interest, focusing only on business and material values.

Viral content, security and privacy issues, lack of quality services, dangerous applications and uncontrolled games, psychological manipulation, fake news, hate speech, copyright violations could be mentioned just as few of consequences, which could affect us in an unregulated environment. In such circumstances, I propose to think to some questions: Does unregulated Internet really mean the free Internet? Does the free Internet is really the bet? Does internet players have enough moral qualities to be able to oppose the new challenges? I think no, that's why I think that by establishing of clear rules, adoption of common standards and by introducing of control technics and authorities we could prevent the harm, and regulation of OTT could impose itself as a way of combating cybercrimes.

To be more convincing about the need to adopt regulatory rules for the OTT, I will outline just some of the potential impacts and risks that may arise because of the lack of regulation.

3.1. Security issues

A number of OTT communication solutions do not support encryption. This implies that attackers can easily eavesdrop into an OTT service (such as VoIP conversation and IM services). Since such applications rely on phone numbers, a lot of specialist explore the feasibility, automation, and scalability of phishing attacks that can be carried out by abusing a phone number. As result, it is demonstrated that the novel system takes a potential victim's phone number as an input, leverages information from applications like Truecaller and Facebook about the victim and his / her social network, checks the presence of phone number's owner (victim) on the attack channels (over-the-top or OTT messaging applications, voice, e-mail, or SMS), and finally targets the victim on the chosen channel. As a proof of concept, taking a random pool of 1.16 million phone numbers, was presented that social and spear phishing attacks can be launched against 51,409 and 180,000 users respectively. Furthermore, voice phishing or vishing attacks can be launched against 722,696 users. Also, found 91,487 highly attractive targets who can be attacked by crafting whaling attacks.

Supplementary, was established that social (69.2%) and spear (54.3%) phishing attacks are more successful than non-targeted phishing attacks (35.5%) on OTT messaging applications. Although similar results were found for other mediums like e-mail, was demonstrated that due to the significantly increased user engagement via new communication applications and the ease with which phone numbers allow collection of information necessary for these attacks, there is a clear need for better protection of OTT messaging applications and development of new regulations .

3.2. Over-The-Top (OTT) bypass fraud

Over-The-Top (OTT) bypass fraud, a recent form of interconnect telecom fraud. In OTT bypass, a normal phone call is diverted over IP to a voice chat application on a smartphone, instead of being terminated over the normal telecom infrastructure. This rerouting (or hijack) is performed by an international transit operator in coordination with the OTT service provider, but without explicit authorization from the caller, callee and their operators. By doing so, they collect a large share of the call charge and induce a significant loss of revenue to the bypassed operators. Moreover, this practice degrades the quality of service without providing any benefits for the users [15].

By, this article, we state that OTT bypass is illegal. Firstly, a call to a certain phone number has to be routed to the operator to which the phone number was allocated by International Telecommunication Union (ITU) or national regulators. This is violated by OTT bypass, because the call is routed to the OTT provider instead. Moreover, most countries impose regulatory fees and taxes for incoming international calls. These are paid by the caller, but hijacked by the bypassing operator. Service level agreements between operators are also violated when an operator pays for a premium quality call route, but its calls are bypassed over the OTT network. Unlike many OTT services, OTT bypass has almost no benefits for the users. In practice, OTT bypass is similar (in its effects) to other types of interconnect bypass fraud, such as simbox bypass [16]. More than that, ITU recently created a working group to study OTT Bypass, where OTT bypass is clearly reported as a fraud [17].

3.3. Confidentiality of communications

Traffic analysis, used by OTT players could help in determining who is talking to whom. Such information can be beneficial to cyber criminals preparing an attack, e.g. for committing corporate espionage or personal attack [3].

3.4. Privacy risks

Some OTT services collect users' private information for commercial gains without making the customer fully aware of the exact details. There is also lack of thorough check on risk assessment and vulnerability levels of applications developed for the OTT market [3].

One issue that should concern all OTT users is the terms of service and end user agreements imposed by OTTs. A study shows that almost 70% of participants never pay attention to the terms of agreements and privacy policies while installing applications on their phones [18]. Moreover, it is impractical for users to read and understand the terms of service agreements of all the applications they are using. As a result, OTT users may unknowingly accept terms of use that come with the end user agreements or default application settings, that's why we think that bu providing common standards and regulations we can prevent appearance of privacy risks.

There are other vulnerability vectors such as use of application with tracking option on, which may pose a threat to national governments.

3.5. Internet manipulation

Internet manipulation may be conducted by internet based content, applications or services for purposes of propaganda, discretization, harming corporate or political competitors, improving personal or brand reputation or plain trolling among other things. To accomplish these objectives, online influencers, hired professionals and/or software − typically Internet bots such as social bots, votebots and clickbots − may be used [5].

3.6. Uncontrolled on-line games

Regardless of whether they are played on a mobile device, gaming console, or computer, video games have become somewhat of a daily ritual for many people. Unfortunately, not all people understand that online games can pose real risks to their personality, health, or social relationships. More and more opinions say that a prolonged and uncontrolled use of video games may cause gamers to experience serious psychological and physical effects including irritability, insomnia, sadness, anxiety, aggressiveness, depression, fatigue, loss of appetite, and discomfort [11]. Moreover, the daily victims confirm in the near future psychologists' predictions. Blue Whale Game, Roblox Game, My Friend Cayla Doll are just a few of the games that can be listed as fatal hazard games.

More than that, we have to take in account psychological construction of human being and as a consequence construction of internet environment. People tend to manipulated and attracted by forbidden things, so the internet is a parallel copy of the real world, not regulating, it can turn into dark area. Provided thesis, is confirmed not just from philosophical manner but also from psychological perspective, and last studies, mentioned more frequently, that content that evokes more anger or amusement is more likely to be shared, and this is driven by the level of activation it induces [9].

Providing real time, interactive Internet based content, applications and services for diverse players and environments is a great challenge for our time. We recognize that, in today's information environment, OTT plays a sizable role in facilitating communications, providing services and access content in our everyday life. In some circumstances, however, we recognize that the risk of malicious actors seeking to use Internet based content, applications and services to mislead people or otherwise promote inauthentic communications can be higher.

Information operations can affect the entire information ecosystem, from individual consumers of information and political parties to governments, civil society organizations, and media companies. An effective response, therefore, requires a whole-of-society approach that features collaboration on matters of security, education, governance, and media literacy [8].

As a consequence to the above mentioned, we could consider that together with technical development, regulation of OTT could impose itself as a way of combating cybercrimes.

4. What we have now on OTT regulations?

4.1. International Telecommunications Union (ITU) efforts

Recognizing the worldwide role of Internet based content, applications and services, the International Telecommunications Union (ITU) has initiated first steppes in providing general rules for OTT regulations. As result, in 2016 the study group appointed, adopted a communication encouraging governments to develop measures to strike an "effective balance" between OTT communications services and traditional communications services, in order to ensure a "level playing field" e.g., with respect to licensing, pricing and charging, universal service, quality of service, security and data protection, interconnection and interoperability, legal interception, taxation, and consumer protection.

They requested a fair level playing field and that OTT players has to be imposed as subject to the same regulations as those of the telecoms sector, when providing equivalent service.

In May 2017, ITU Council Working Group on International Internet-related Public Policy Issues (CWG-Internet) launched an open online and physical consultation on OTTs. The working group has evaluated opportunities and implications associated with OTT including policy and regulatory matters. It considers regulatory approaches for OTTs that ensure security, safety and privacy of the consumer and will work towards developing model partnership agreements for cooperation at the local and international level.

The physical consultation took place in September and received inputs from a wide range of stakeholders. During the World Telecommunications Development Conference (WTDC)—the main conference of the ITU's Development sector, ITU-D—which took place in Argentina during October 2017, several governments have sought to expand the ITU Internet public policy mandate. As we approach the ITU's 2018 Plenipotentiary Conference, or "Plenipot" we can expect conversations on regulatory frameworks to escalate in the ITU [10].

4.2. European Union's overview on OTT regulations

At European level, until now, we do not have a common understanding and unique regulation designed for OTT field. However, as part of its Digital Single Market Strategy, the European Commission is currently reviewing the EU telecoms framework. In September 2015, the Commission launched a public consultation, inviting stakeholders to submit their views on the existing rules and on possible alterations. As a tentative for clarification, BEREC present in 2015 a Report with regard to OTT services, by which provide some classification of OTT and provide some views regard potential future regulation. For the moment, BEREC refuse to accept completely, the idea that OTT present totally new realities, and they could not be assimilated to other services. There are for, they present a classification of OTT's, which was proposed to be put on the basis of future regulations. Having in mind the idea of equity and equal regulation, BEREC propose to distinguish OTT varieties as follow:

OTT-0: an OTT service that qualifies as an ECS;

OTT-1: an OTT service that is not an ECS but potentially competes with an ECS;

OTT-2: other OTT services.

However, more and more voices point that BEREC proposed taxonomy is already outdated and would create even more interpretation problems than the current obsolete ECS. The way forward is building upon IAS and ISS [4].

More than that confusion is generated by different national regulatory framework developed. At European level, certain types of OTT services are qualified, by national regulators, as (publicly available) ECS and, as such, are subject to regulation under current EU telecommunications laws. For example, in most (if not all) EU member states, Voice over IP (VoIP) services providing for a break-out to the public telephony network (PSTN) are considered regulated telecommunication services. BEREC qualifies these services as OTT-0. The OTT Report notes, however, that the scope of the ECS definition provided for in the Framework Directive (2002/21/EC) is not sufficiently clear. BEREC therefore suggests to clarify the definition of ECS to ensure that "it keeps pace with the current developments". BEREC also notes that the lack of clarity allowing for different interpretations of the ECS definition leads to a lack of harmonization between members states in assessing which OTT services constitute ECS. The classification as an ECS triggers the applicability of obligations such as emergency calling, safeguarding telecommunications secrecy, and telecommunications-specific consumer protection rules [1].

Unlike BEREC, the German Federal Network Agency holds the existing regulatory framework for ECS is yet applicable to certain types of OTT services. In the Cologne proceedings, the German regulator argued that Google is involved in the establishment of the connection and therefore responsible for the conveyance of signals.

More than that, Germany as well Russia, propose legislation that would require the owners social media companies networks and messengers to delete any “illegal content” within 24 hours, or they would face steep fines. In cases where the content isn’t clearly illegal, social networks can take up to a week to review a complaint. Social media companies face fines as high as $57 million if they do not comply with the new law.

In the media it is announced, that France is the next country which is ready to adopt a new social media law during the next period of time. In this circumstances, the European Commission could be force to take actions and go far with Internet based content, applications and services regulation.

4.3. Other OTT regulation practices

In August 2017, the Indonesian government via the Ministry of Communication and Informatics (MCI) unveiled a liability framework for OTT providers. The sweeping regulations cover a whole slew of companies including SMS and voice calls and email services, chatting and instant messaging platforms, financial and commercial transaction service providers, search engines, social network and online media delivery networks, and companies that store and mine online data. The regulation, which is currently under review, makes it mandatory for offshore businesses to establish a "permanent establishment" either through fixed local premises or by employing locals in their operations in Indonesia. Transnational companies are also required to have an agreement with an Indonesian network provider, and use local IP numbers and national payment gateways for their services [10].

Similar efforts to regulate online platforms are underway in Thailand. The National Broadcasting and Telecommunications Commission (NBTC) has committed to create a "level playing field" between OTT service providers and traditional broadcasting and telecommunications industries. In

April 2017, it suggested introducing bandwidth fees for online content providers, and has also proposed bringing OTT service providers under an operating license framework, taxing them for transactions by local merchants and making them liable for illegal content. In July 2017, the Thai government issued an ultimatum to OTT services to register with the national telecom regulator or face getting slapped with sanctions such as bans on advertising that would threaten revenue growth [10].

In Latin America, several countries including Uruguay, Costa Rica, Colombia, Argentina and Brazil are considering legislative changes to enable the taxing of OTT players. In Argentina, the government has issued a set of principles for telecommunications regulation that create obligations for registration of Internet intermediaries. Ahead of the Presidential elections in 2018 and with mounting opposition to his regime, the Zimbabwean President Robert Mugabe has created a Cyber Security, Threat Detection, and Mitigation Ministry to reign in threats emanating from social media. The government is also pressing ahead with a Computer and Cyber Crimes Bill, a comprehensive legislation that would allow the police to intercept data, seize electronic equipment and arrest people on loosely defined charges of "insurgency" and "terrorism" [10].

5. Future developments

Information presented above shows that regulation of internet based content, applications and services present itself as an actual discussion with many questions but few answers. However, we have many opinions evoked, we do not have a clear picture of internet-based content, applications and services which we have to regulate. For the moment, we have a huge variety of services and applications and forms of content providing (voice services, hosting services, email services instant messaging, web-based content, news sites, social media, search engines, video and multimedia content) but we do not have a common understanding of classification and assimilation of them. In such a way, clear identification of the content, applications, and services we intend to regulate must be set as a priority in the succession of the actions we are proposing to make.

Is clear that OTT services are new realities, which will affect our future existence, and work, that is why to build a future in old soul, I think is a wrong way, is better to create something new, which will work for future than just to adapt something that will be a solution for the moment. We should promote new regulations, which will be designed special for new realities and then to adapt it to new challenges in case if they will appear during the time. More than that, we have to take in account that summing of all internet based content, applications and services in one big reality could imposed itself as an impossible exercise, grace to their variety, that's why when we think to new regulation we have to think to different internet players dealing with administration of different content, application and services. The regulations should take into account the type of service and the rights to be protected in a differentiated and specific way. Services offered by travel agencies, financial institutions, property rentals, or those providing alternative local transport considered as public services, should not be regulated in the same way. However, we have to create a common legal foundation for entire internet-based content, applications and services field by introducing general principles linked assurance of fundamental human rights, security and contribute to equal development of all internet players.

Not having a unique jurisdiction of internet, we have to concentrate our efforts by concentrating efforts of all stakeholders in the same direction regardless of country or authority. The new legislation should not separate the interests of the communications companies from those of the OTT, but has to be develop in a way, as by it to contribute to promotion of cooperation between all

internet players and do not affect the interests of users. However, self-regulation, standardization certification inclusive philological certification should be promoted at all levels, or they could prevent harms and assure wellbeing.

Concluding, we can certainly mention that for the moment we face new internet realities linked to Internet-based content, applications and services provided. We agree that, during the last period, our common understanding of internet was changed, and common construction of World Wide Web is destroyed, we have new realities, new players, new requirements and new challenges, and as a consequence we have to find new concepts, new rules and new control and cooperation forms and by this way to be able to combat new form of risks and infringements.

6. References

[1] BACKER, MCKENZIE, EU intends to regulate Over-the-Top ("OTT") services, Germany 2016. Available at: http://www.bakermckenzie.com/-/media/files/insight/publications/2016/03/eu-intends-to-regulate-over-the-top-ott-services/al_germany_regulateottservices_mar16.pdf?la=en[Accessed 14 Dec. 2017].

[2] BEREC, Report on OTT services, 2016.BoR (16)35. Available at: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services [Accessed 14 Dec. 2017].

[3] COMMONWEALTH TELECOMMUNICATIONS ORGANIZATION, Research Study, The Dynamics of Over-The-Top (OTT) Services, 2016. Available at: http://www.cto.int/media/CTOOTTStudyPaperFinal_ReviewedDraft04Oct2016.pdf [Accessed 14 Dec. 2017].

[4] ETNO Response to the Public Consultation on the draft BEREC Report on OTT services BoR (15) 142, 2015. Available at: https://etno.eu/datas/positions-papers/2015/Reflection-Documents/RD418%20-%20BEREC%20OTT%20services.pdf [Accessed 14 Dec. 2017].

[5] "Internet Manipulation." Wikipedia. Wikimedia Foundation, Available at: https://en.wikipedia.org/wiki/Internet_manipulation[Accessed 14 Dec. 2017].

[6] "Introduction to OTT", OTT Source. N.p., 22 Mar. 2013. Web. Available at: http://ottsource.com/ott-tutorials/introduction-to-ott/ [Accessed 14 Dec. 2017].

[7] PALLERO, J., JIT SINGH CHIMA R., Proposals for regulating internet apps and services: understanding the digital rights impact of the "Over-the-top", 2017. Available at: https://www.accessnow.org/cms/assets/uploads/2017/08/Access_Now_OTT-position%E2%80%93paper.pdf [Accessed 14 Dec. 2017].

[8] WEEDON, J., NULAND, W., STAMOS A., Information Operations and Facebook, in: Information Operations and Facebook, 2017. Available at: https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf [Accessed 14 Dec. 2017].

[9] BERGER, J., MILKMAN, K. L., What Makes Online Content Viral? in: Journal of Marketing Research, 2012. Available at: http://jonahberger.com/wp-content/uploads/2013/02/ViralityB.pdf [Accessed 14 Dec. 2017].

[10] PANDAY, J., An Over-The-Top Approach to Internet Regulation in Developing Countries, in: 2017 revised draft OTT regulation (Indonesia), 2017. Available at: https://www.eff.org/deeplinks/2017/10/over-top-approach-internet-regulation-developing-countries [Accessed 14 Dec. 2017].

[11] LI, W., & ANTHONY, B. (In press), Internet and Video Game Addiction, in: Oxford Bibliographies in Social Work. Ed. Edward J. Mullen. New York: Oxford University Press.

[12] "Over-the-top Media Services", Wikipedia. Wikimedia Foundation. Available at: https://en.wikipedia.org/wiki/Over-the-top_media_services [Accessed 14 Dec. 2017].

[13] Policy Department A: Economic and Scientific policy, Over-the-Top players (OTTs), Directorate General for Internal Policies, European Parliament, 2015. PE 569.979.

[14] GUPTA, S., GUPTA, P., AHAMAD, M. and KUMARAGURU, P., Abusing phone numbers and cross-application features for crafting, targeted attacks, in CoRR, abs/1512.07330, 2015. Available at: https://arxiv.org/abs/1512.07330v1[Accessed 14 Dec. 2017].

[15] SAHIN, Merve, Over-The-Top Bypass: Study of a Recent Telephony Fraud. Available at: http://s3.eurecom.fr/docs/ccs16_sahin.pdf [Accessed 14 Dec. 2017].

[16] REAVES, B., SHERNAN, E., BATES, A., CARTER, H., and TRAYNOR, P., Blocking cellular interconnect bypass fraud at the network edge, in USENIX Security, 2015.

[17] ITU Study Group 3, Question 9/3. Ott bypass. International Telecommunication Union. Available at: https://www.itu.int/itu-t/workprog/wp item.aspx?isn=10892#TOP.

[18] CHIN, E., FELT, A. P., SEKAR, V., and WAGNER, D., Measuring user confidence in smartphone security and privacy, in SOUPS ’12, 2012.

.