ANALYSIS OF INTERNET CONTENT REGULATIONS IN TURKEY. ANALYTICAL SURVEY OF THE ISSUES AND LITERATURE

Arif ARISOY

Candidate Number: 95624

ANALYSIS OF INTERNET CONTENT REGULATIONS IN TURKEY. ANALYTICAL SURVEY OF THE ISSUES AND LITERATURE

Candidate Number: 95624

SUMMARY

This dissertation is devoted to the study of the Internet regulations in Turkey. I will start by introducing what kinds of changes Internet has made in recent years in order to show the concerns of regulators and related actors. A study of censorship and a comparative analysis of online regulations of several countries will then follow. The characteristics of those countries' regulatory systems will be used to make policy suggestions for Turkish policymakers. Findings of this chapter suggest that there are several issues which need to be considered primarily, such as freedom of expression, infringement of intellectual property rights and obscenity and parental control. For this reason, I will extend the discussion to include the opinions of different parties including academics, activists and professionals on those issues. The following chapter focuses on the milestones of online content regulations in Turkey. The findings of the previous chapters will be the basis for evaluation of Turkey's online content regulations. We shall see in the conclusion that despite the fact that there have been debates over the transparency of Turkish regulations, the country can be classified as a moderate censor along with a number of developed countries including the United Kingdom, The United States of America and Australia.

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Prof Ed Steinmueller for his kind guidance and support throughout my studies. I am very grateful that I had a chance to study with him. His wisdom and precious suggestions shaped this dissertation.

I also would like to express my gratitude to my supervisor, Dr James Revill for his support and tireless efforts to keep the concept of this research simple and concentrate on the questions at hand. His encouragement and positivity has been a great motivation for me.

And of course I am indebted to my wife, Derya and my baby daughter, Amine Nisa for their great patience and understanding. Thank you very much for your valuable presence in my life.

TABLE OF CONTENTS

ABBREVIATIONS

ACLU	American Civil Liberties Union
ACMA	The Australian Media and Communication Authority
AIO	Alternative Informatics Organization
AOL	America Online
BSA	Business Software Alliance
CDA	Communications Decency Act
DNS	Domain Name Server
DPI	Deep Packet Inspection
EPIC	Electronic Privacy Information Centre
HADOPI	Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet
HRW	Human Rights Watch
HTTP	Hyper Text Transfer Protocol
ICTA	The Information and Communication Technologies Authority
ICTRC	Iran's Civil Society Organizations Training and Research Centre
ICTs	Information and Communication Technologies
IDC	International Data Corporation
IFPI	The International Federation of the Phonographic Industry
IP	Internet Protocol
IPR	Intellectual Property Rights
ISP	Internet Service Provider
ITU	International Telecommunication Union
IWF	The Internet Watch Foundation
MPAA	Motion Picture Association America
MUYAP	Turkish Phonographic Industry Society
NGO	Non-Governmental Organization
P2P	Peer to Peer
R&D	Research and Development
RC	Refused Classification
RTUK	Radio and Television Supreme Council of Turkey
SOPA	Stop Online Piracy Act
TIB	Telecommunications Presidency

TPC	Turkish Penal Code
UN	United Nations
URL	Uniform Resource Locator
USITC	United States International Trade Commission
VPN	Virtual Private Network

PREFACE

In this study, the research question concerns how Turkish policy makers should proceed with online content regulations. In order to answer this question, a secondary question has been introduced which is: What are the noteworthy characteristics of some countries' regulations on issues, such as pornography or freedom of expression? This study consists of five parts. Firstly a literature review has been carried out regarding to basic concepts on a very broad range from censorship, pornography, freedom of expression to the regulations of several countries including the United States of America, the United Kingdom, the Islamic Republic of Iran and Australia. During the literature review, some empirical studies on the effects of infringement of intellectual property rights on the industry, effects of obscenity on minors and adults have been studied. Also reports of several organizations such as UN Human Rights Council, Human Rights Watch, Organization for Security and Co-operation in Europe have been investigated. Secondly, a censorship scale has been developed in order to classify countries according to their attempts to regulate online environment. This comparison is essential to find out answers to our secondary research question. Then thirdly, opinions of different actors on the key topics of online content regulations are discussed. After introducing the existing picture of Turkey's online regulations trajectory, some policy suggestions are given. In the conclusion chapter censorship evaluation result of the country is presented. Guidance and advises of my supervisors, Prof Ed Steinmueller and Dr James Revill contributed very much to the structure of this study.

1. INTRODUCTION

The Internet has fundamentally changed the way people communicate with each other. Global communication has never been faster and easier. Social networking websites made it possible to organize thousands of friends in a minute for an uprising, party or a riot. The democratic movements in the Middle East and North Africa appear to have been facilitated by the fast and easy communication provided by the Internet. People still meet their friends at cafes, parties or clubs, but the Internet has created new opportunities to find other people who share the same interests or concerns. Even if the interests are about the most extreme or obscure topics such as the impact of 15th century poetry in Ottoman Empire or Queen Elizabeth's diet program, there is probably a Facebook group about it. Moreover, email which is one of the most popular uses of the Internet has almost replaced personal postal mail sending, as it promises pace and easiness. Unlike letters which can reach only one person or one place at a time, email has made life much easier by providing multiple recipient, blind carbon copy and file attachment capabilities. Furthermore new ways of interactions emerged such as video and audio conferencing, chat groups and online communities where people can even share previously unthinkable experiences.

The Internet has also changed the way that people interact with information. Search engines, which help people find the information, images and videos on the net, have become an indispensable part of our lives. Although they created an illusion that the answer is on the Internet to whatever question, search engines have proved useful tools for daily lives. Housewives seeking for exotic pie recipes or drivers who do not know what to do when their cars are broken on the road frequently do online searches. However the relevance and the correctness of the findings for more serious searches is another issue, since the Internet is not capable of understanding the nature of knowledge. When confronted a research problem, students instinctively do Google searches to get the information rather than going to the library and struggling with heavy books. Despite the best efforts of teachers to discourage 'copying and pasting' text from the Internet into their essays without recognition of the source, students prefer the information they find via search engines to complete their projects without checking the accuracy and the reasoning to verify facts.

The Internet has also made many changes in the way that business is organised. For example, the Internet has made it possible to introduce new business models such as e-commerce.

Thanks to the ability to reach anybody anywhere in the world with a simple click of the mouse, companies enjoyed new communication channels to spread their business into every corner of the earth. On the other hand, online technologies have not only provided opportunities to companies, but also given chance to customers to be involved in the decision making processes. Ten years ago customers had to buy whatever the Toyota designers came up with. Nowadays they can actually contribute to the design process by providing feedbacks from the company's website or social media page. The communication, information and business issues mentioned above are only a few of the changes that the Internet has facilitated.

However, it would be an optimistic view to claim that Internet did nothing but increased the quality of lives. Along with its benefits, new challenges such as the infringement of intellectual property rights (IPR), invasion of privacy and cyber warfare have occurred and proliferated rapidly. Peer to peer (p2p) applications, which provide Internet users with opportunities to easily locate shared files on another computer connected to the network and to download the data to users' own computers, are now being used by millions of people to reproduce and distribute copyrighted content without permission. Right holders claim that this powerful architecture of the Intemet supports intellectual property rights infringement which hit the film and music industry so badly that the content owners are feeling threatened and many people have even come face to face with job losses. A few empirical studies show considerable job losses associated with infringement of IPR. A BSA and IDC study states that 'a decrease in the piracy rate from 43 percent to 33 percent in the countries covered by the study would result in an additional 500.000 jobs in those countries.' (USITC, 2011:58) However, one might argue that the real problem is the failure of the industry to make legal means of accessing music and other copyrighted content.

In addition, malicious software and spam emails which are the popular aspects of the dark side of the Intemet are not only disturbing individuals, but also threatening their privacy by providing backdoors to hackers. People who do not know that their security defences are being breached and control of their personal computers ceded to malicious parties become zombies and networks of such private computers infected with malicious software and controlled as a group without the owners' knowledge, which are called bot-nets, get bigger. As many people do not know how to protect their personal computers against online threats, bot-net owners who control a number of zombie computers exploit those weaknesses to expand their zombie networks that are being used either to distribute malicious content or attack many institutions such as government agencies, private companies and banks where privacy has serious monetary value.

To make things worse, since banks, universities and numerous institutions tend to use more and more information and communication technologies (ICTs) nowadays, whether to reduce the costs of human resources or to be more technologically polished, and the online platforms in which services are delivered are being attacked by many criminals, the number of incidents which involve victims whose privacy were severely violated is increasing. US Defence Secretary Leon Panetta told an audience at the McConnell Centre at the University of Lousville that we are literally getting hundreds or thousands of attacks every day that try to exploit information in various agencies or departments. There are plenty of targets beyond government, too.' Also, according to the 2011 Second Annual Cost of Cybercrime Study by the Ponemon Institute, the average cost of malicious activities on the Internet is up 56% on previous year's figures.

Moreover, some features of the Internet are like a double edge sword which has the ability to empower and destroy at the same time. The sense of anonymity is a wonderful facilitator which can encourage shy people to participate in a discussion group or to create a blog in which he or she can share the brightest ideas without the fear of social rejection. On the other hand, the disguises which were offered by this advanced global network and programs such as Tor, which assist users conceal their locations or anonymize online activities, help them cross social boundaries and, for example, become sexual offenders.

One of the most significant issues of those dark side online actions is child abuse, because the Internet facilitated the connections between the existing threats and children. Considering that criminals always adapt to technological changes, it is not a very surprising fact that paedophiles exploit the new technological facilitators to prey on young people and network with the like-minded people to distribute sexually explicit material. Because of that, along with many other reasons, governments try to regulate the Internet all over the world and those attempts spark the hottest debates. Because, according to some civil liberties organisations such as American Civil Liberties Union (ACLU), Electronic Privacy Information Centre (EPIC), governments are using protection of kids and other issues mentioned above as an excuse for 'ill-conceived censorship schemes.' (Akdeniz, 2001:258) They also argue that no matter what types of filtering techniques are used, children will always find a way around to reach to the websites which are nothing more than the reflections of the real world. So what really matters is teaching kids how to surf safely and avoid suspicious things, as they should do in real life, too. Also, according to the advocates of this perspective, the Internet's success comes from its free environment where everybody can speak their mind without being judged or reprimanded for their words. In other words, government intervention on the Internet is nothing but censorship which threatens its free atmosphere, undermines every good aspect of it and leads to catastrophic consequences, as the freedom of expression, which is a fundamental right, is seriously violated.

On the other hand, there are some people who claim that the Internet is no different from other electronic media such as television and radio. It is just another way of accessing information or communicating with others. Given that broadcasting pornography or selling harmful substances on television is unacceptable, there is no rationale for facilitating similar activities conducted in cyberspace. It is important to underline the fact that the Internet is different from television to some extent, as one must take greater action to select messages on cyberspace. However there are less control mechanisms on the Internet. All kinds of pornography including animal abuse and sexual solicitation of children exist in some volume on the net. Many children have come across such websites, whether intentionally or accidentally, which can sometimes cause serious psychological problems such as addiction, isolation, unhealthy interference with normal sexual development, imitation of inappropriate behaviours, stimulation of premature sexual activity, increased aggression, distorted beliefs and perceptions and neglecting other areas of their lives. (Maltz & Maltz, 2006:72, Benedek & Brown, 1999:238) So given that even in real life the speech which provokes violence, induces fear and panic such as shouting bomb on an aeroplane is not protected by the law, online activities should be treated consistently with existing laws and governments should enact new laws if necessary to make sure there is consistency.

The research question of this study is *how Turkish policy makers should proceed with online regulations.* The government enacted Law No. 5651 entitled 'Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting' in 2007 and launched a free and optional filtering service called the Safer Internet Service in 2011. The

former categorizes the online offenses and requires ISPs to block the websites which host content related to the promotion of prostitution, providing place and opportunity for gambling, sexual abuse of children, encouraging people to commit suicide, supplying drugs which are dangerous for health. The latter provides Internet users with two profiles called Family and Child and the Internet service of those who want to benefit from the Safer Internet is filtered according to predefined parameters. Details of both of the legislations, liabilities of actors, technical and social challenges, major issues and society's response will be discussed in the fourth chapter entitled Analysis of Online Content Regulations in Turkey. Before that, in the following chapter a secondary research question will be studied, which is: *What are the noteworthy characteristics of some countries' regulations on issues, such as pornography or freedom of expression?* This contextual information is useful in informing expectations of how online content will be regulated. In order to answer this question, an international comparison of online regulations will be made within the context of a censorship scale. Those characteristics will help determine the issues that Turkish policy makers should consider in future regulations.

After that some important topics will be investigated such as Freedom of Speech, infringement of IPR and obscenity in the chapter entitled The Debate. In this chapter, arguments of academics, activists and related actors will be discussed in order to evaluate Turkish policy makers' concerns on those matters from different perspectives.

The next chapter will be about the details of Turkey's attempts to regulate online activities. Those regulations will be evaluated according to the findings of previous chapters and lastly in the conclusion chapter, policy suggestions will be presented along with the censorship evaluation result of the country.

2. CENSORSHIP AND COMPARISON OF WORLDWIDE INTERNET CONTENT REGULATIONS

In this chapter, different perspectives and approaches to the notion of censorship will be discussed. Firstly a censorship scale will be defined. After that different countries which have noteworthy online regulation characteristics will be studied. Lastly the findings of country analysis will be given. These findings are vital for the research question of this dissertation.

In general, censorship is the editing and removing the material which is considered to be harmful, offensive or inconvenient to the intended audience by governments or regulatory bodies. For many people in Western culture, censorship is a pejorative term which has meaning beyond editing or removal. Television, radio, books, music, the press and the Internet are all subject to regulations because of variety of reasons. Protection of children and family values by controlling obscenity, pornography and violence and securing military secrets in any written or visual presentation are always at the top of the list, followed by restricting hate speech against any part of the society, protecting intellectual property rights and so on. Among the most common historical rationales are political, religious, moral and social and what they have in common is a claim that the public interest will be negatively affected by the communication and censors try to justify their actions by underlining the protection of public welfare. (Marx, 2001:1584)

Censorship of the Internet occurs with the same motives and decision processes but with very different ways of implementing and enforcing regulation, as it does in the traditional media. It has its own characteristics, as there are no national borders and the way information is broadcasted is different. Governments might have legal control over the content of the websites which are hosted within the country, but when it comes to the foreign websites new challenges occur. Sometimes in order to ban access to an inappropriate content, the entire website has to be blocked and this is not an effective method, as there are many proxy servers which help users circumvent the filtering. That challenge leads governments invest heavily in finding more comprehensive ways of filtering which also limit access to mediators helping people route around. China, Cuba, Vietnam, Iran, North Korea, Saudi Arabia are the countries which have the most extensive filtering practices and those nations along with others 'primarily fall in three regions: East Asia, the Middle East and North Africa and Central Asia.' (Dutton et al., 2011:43) There is a common agreement that China has one of the most sophisticated and pervasive filtering systems of the Internet censorship, followed by Vietnam which applies basically the same practices. Myanmar, which famously shut down the Internet countrywide in autumn 2007 during the disturbances, is worth mentioning, too. (Dutton et al., 2011:44)

Policy makers in different countries are looking at the censorship concept from different perspectives. Priorities differ according to many criteria and social structure. Before highlighting some of the countries, ranging from the most liberal ones to strict regimes, and their applications, the concept of censorship will be investigated under three categories in the following section in order to create a censorship scale and evaluate those countries. Those categories are Libertarians, Moderates and Extremists. Objectors claim that, whatever the reason is, filtering cannot be justified. Moderates highlight the certain circumstances and argue that filtering can be a part of overall solution, whereas advocates of extreme perspective appreciate censorship to protect political, social or even personal interests.

2.1 Censorship: Perspectives and Differences

2.1.1 Libertarians

For some people even the smallest form of selective presentation is censorship and cannot be accepted. According to libertarians, considering that free speech is the vital and indispensable element for the democracy, surveillance and suppression of any personal communication cannot be justified, whether it is for enhancing social solidarity by avoiding insults to shared values or protecting national interests. Advocates of libertarian constituency claim that any attempt to withhold, masquerade or edit information by governments is an attack to the fundamentals of the free society. The advocates of this perspective state that a set of criteria used to establish the level of obscenity, sedition, fraud and incivility in media is beneficial to the wellbeing of the public. For instance, the Federal Trade Commission's famous regulation entitled Truth in Advertising was enacted to protect consumers from fraudulent or deceptive commercial communication. However 'lawful restrictions for exposure based on said criteria and set by any organization other than individual's own legal guardian, whether it be a parent or otherwise, and henceforth referred to as a parent, are unethical' (Reinhard, 2007:165)

For instance, government agencies like the Motion Picture Association of America (MPAA) or Radio and Television Supreme Council of Turkey (RTÜK) are responsible for determining what content is appropriate for children, and what content should be classified as obscenity and therefore inappropriate for children. In other words, they advise responsible parents against allowing their children to view objectionable material. Warning the TV audience with a message like 'This show contains scenes that some viewers may find disturbing' or classifying adult websites under the .xxx extension is the result of such attempts. Given that governments are not capable of assessing the individual reactions people have to specific content, that advisory duty should not extend to determining the age at which an individual is mature enough to legally access such content. It is a parent's duty to raise their child, and not the government's. (Reinhard, 2007:166) This approach is plausible, as it underlines the importance of rating systems and parental control.

On the other hand, given that this approach does not provide an effective control mechanism for the protection of children in absence of parents and underestimate the importance of key issues such as public safety and order, based on the argument that governments use those words to mask their desires to censor which would not otherwise be legally supported, it would be a very optimistic view to agree that this is the right and adequate way of dealing with the complexity of modern issues. That might be one of the underlying reasons for the fact that even in the most liberal countries policy makers are in pursuit of more comprehensive ways to address these issues. Nevertheless setting criteria for media and maintaining content rating systems should be considered as important components of the ultimate solution.

2.1.2 Moderates

Countries mostly cluster in the second category in which freedom of expression is highly appreciated; however its extension without limit is questioned. From this perspective 'it is argued that that the right to exercise free expression does not include the right to do unjustifiable harm to others. Citizens have a right to freedom of expression, but the state can limit that right in order to prevent a threat to public order, the security of the state, or third parties in need of protection such as children. Rights are costly, and someone must pay for them.' (Almagor, 2006:13) Those who pay for the harmful actions of others are not always individuals, but sometimes companies or even industries. For example, according to the BBC news on 30 April 2012, the Swedish website The Pirate Bay which hosts links to download mostly pirated music, movie and e-book files was blocked throughout the UK, as it is claimed to destroy jobs and undermine investment in new British artists. The website was also blocked in several European countries such as France, too. Along with many others, pirate websites are considered to be one of the biggest challenges industries have faced so far. Because creating copies of published books can be done by a single scanner and a computer. Once the first copy falls into the Internet, it may potentially be downloaded by millions of people in seconds. Sometimes before the publishers launch the e-book versions of the bestsellers, pirates convert scanned copies to e-book format and make them available to the public. That is why copyright holders are constantly are talking with governments and major search engines to find effective ways to combat piracy. The latter do not always respond positively to the demands asking them to ensure pirate websites do not appear at the top of the web searches for people looking for specific keywords.

Policy makers are aware of the severity of the issue. Considering the Pirate Bay case in the UK or notice and take down legislations in France, they obviously do not evaluate this kind of website blocking as censorship or they surrender to the technical challenges of cyber complexity. On the other hand, those platforms are also sharing open source free software or providing communication channels to those who want to talk about their interests and search for answers about the problems of their own. This is where the hottest debates flame, because there are two options according to where the website is hosted. The latest trend in online filtering is contacting the content provider to remove illegal content. If authorities cannot reach to content providers or their request for removal of such content is rejected or ignored, the website is blocked at ISP level. Domestic websites or all kinds of online applications might be subject to this notice and take down legislations. If the objectionable content is hosted outside of the country, due to cross border jurisdiction problems, most of the time there is no way other than blocking the entire platform without any notice. Unless the content provider removes the objectionable part himself, it is really a technical challenge to remove only a part of the content at ISP level, which requires extensive investment in deep packet inspection capabilities whose necessity and efficiency need to be studied carefully; because that also means surveillance of the Internet traffic by ISPs.

Moreover in moderate censorship approach, pornography, hate speech, violation of moral and social values and national security are taken into consideration more seriously. However there is not a collective agreement on that matter. Content which is found objectionable in one country is not necessarily considered as harmful or illegal in another. Below some examples of this argument are given. Further examples will be investigated in the Country Ratings section.

In the UK, extreme pornographic images that depict acts which threaten a person's life, acts which result in or are likely to result in serious injury to a person's anus, breasts or genitals, bestiality or necrophilia, is illegal to possess as of 2009, carrying a three year imprisonment. Possession of hardcore pornography for private use is not an offence and sale or distribution of such content to minors under 18 is prohibited. Except for child pornography, UK citizens can access to hardcore pornography on web sites and magazines.

Australia has a different and detailed content classification system which is established by Australian Communications and Media Authority. Websites or images which fall under Refused Classification (RC) which includes child pornography and bestiality are illegal to broadcast. Production, dissemination and consumption of illegal internet pornography is subject to criminal legislation.

In addition, while countries such as Germany, France, and Austria criminalize the denial of the Jewish Holocaust, not all the member states of the European Union or Council of Europe criminalize such conduct or content. (Akdeniz, 2010: 261) A well known Holocaust denier Fredrick Töben was arrested at the Heathrow Airport by British Police because of a pending European arrest warrant issued by the German authorities. The warrant was issued because of Töben's writings on his website denying the existence of the Jewish Holocaust under Hitler. This is a good example which proves that certain acts may be regarded as offensive or illegal in some countries, but are nevertheless not criminalized by law within certain jurisdictions, and evidently differences exist even between jurisdictions within a country.

The only matter on which countries come to an agreement is protection of minors against harmful content and preventing adults from viewing child pornography. The European Commission in its October 1996 Communication stated that: 'These different categories of content pose radically different issues of principle and call for very different legal and technological responses. It would be dangerous to amalgamate separate issues such as children accessing pornographic content for adults, and adults accessing pornography about children.' (Akdeniz, 2010:262) However it is not easy to reconcile different regulatory perspectives about how this issue has to be managed. For instance, although policy makers of all member states in European Union appreciate multi-player involvement and taking advantage of the expertise of all actors involved as the important factors of a successful co-regulation framework to shield minors from harmful new media content, there is not a complete solution, because different cultures with different jurisprudences exist across Europe. (Lievens, 2007:326, Gevers et al., 2001:372)

Some scholars who subscribe themselves to the necessity of moderate censorship note further aspects of the issue. For example, in order to 'keep competitive forces flowing fairly and smoothly and economy developing, some regulation or systematization over the Internet is necessary. The electronic infrastructure should be monitored to prevent monopolization of the keys to accessing information and to ensure maximum volume and diversity of content.' (Sussman, 2000:542) Although many academics underline the risk of misuse of such regulations leading to excessive censorship and state that the Internet does not need either governmental or corporate monopolies, (Sussman, 2000:542, Bittlingmayer et al., 2002:300, Wong et al., 2011:473) they cannot present a persuasive solution about how to avoid the risks that some are concerned about. This is the major weakness of this perspective.

Another problematic issue is that almost every country has different criterion and content classification systems. Administrative bodies such as ACMA in Australia or Internet hotlines run by the private sector such as Internet Watch Foundation in the UK decide which content or website should be subject to blocking. Therefore decisions for blocking illegal or harmful content are not always taken by the court of law. Some academics oppose to the role given to administrative bodies and public or private Internet hotlines set in many countries, stating that such organizations may not be in a position to judge the suitability or illegality of the online materials, because illegality can only be investigated by the courts of law rather than hotline operators. 'It may be tempting to identify and attempt to block content posted to particular websites, or other Internet forums that seem devoted to illegality, such measures could set dangerous precedents if hotlines or administrative bodies assume the role of the courts. Over time, such an approach could result in a form of privatized censorship with no limit on its application.' (Akdeniz, 2010:269)

To summarize, concerns about the compatibility of blocking actions with the fundamental right of freedom of expression are on the rise. Governments which attempt to identify and block offensive content generally lack convincing answers to the following questions related to transparency and accountability concerns: What is the legal basis of the offensive content classification? How is the criteria defined and who participates in the decision making processes? What are the accountabilities of actors who participate in criteria definition processes or operate the hotlines?

2.1.3 Extremists

Countries, who are trying to eliminate the anti-government activities and 'ideology contamination', are attempting to control all of the information flow. Those can be classified as the extreme censors. In those regimes an authority decides which content is compatible with the current law and which can disrupt social stability and threaten the reputation and interests of the state. China is unsurprisingly one of the most famous countries with extensive censorship legislations. China's political leaders consider the Internet as a great opportunity for the economic growth and prosperity. However they also fear that the price that the country pays for this economic wealth through cyber opportunities will be a downfall of the Chinese Communist Party. (Tan et al., 1997:12, Cheung, 2006:2) Therefore only '*politically correct speech*' to be published on the media, meaning that anti-government content, violence, pornography and expressions of ideas that undermine state religious policy are removed. Also there is an interesting trend with Sina Weibo, the Chinese twitter in which members start with a score of 80 points and have points deducted for mistruths as judged by the administrators of the microblogging site. Moreover, China's Internet Regulations consists of not only website filtering, but also disconnecting offensive users from the network and preventing private sector from maintaining direct links to the outside of the country without being transmitted through government's online traffic surveillance systems. Policy makers try to justify their actions pointing to the consistency of the regulations with the communist style of governance that holds social stability paramount. (Cheung, 2006:3)

The advocates of this category claim that fighting against *social evils* with high costs such as prostitution, abuse of drugs, pornography, gambling and politically offensive materials, which threaten social integrity and national customs, is more important than providing limitless freedom of speech to citizens. Socialist Republic of Vietnam is another country which subscribes itself to this argument. It is argued that the rise of social evils in Vietnam has accelerated since the open door policy and attributed to negative western influences.

(Surborg, 2008:352) It is reported that 'the government blocks access to web sites which are considered to be politically and morally 'dangerous', including foreign news sites and those of human rights organisations set up by Vietnamese abroad.' (Surborg, 2008:351) The article which regulates online content in Vietnam states that 'organizations, individuals providing and using Internet services are responsible for information accessed, transmitted on the Internet.' Along with the other articles the government tries to create a legal basis to take actions against social and political evils, but the term 'responsibility' is not well defined and not only individuals, but also ISPs and content providers are made liable for online offences, too. Such ambiguities might have been put to the legislations intentionally, so that states can discipline the Internet actors by creating a cyber panopticon in which prisoners can neither see the inspector who conducts surveillance from a privileged location nor know when they are being watched. Considering the dispersed nature of online activities and availability of thousands of alternative ways to access information without being captured by the authorities, governments are also aware of the impossibility of controlling all of the information flow and might think that such uncertainties could be partially helpful to preserve the political power.

Although extreme censorship is challenged by the fast globalisation, it is difficult to claim that strict regimes will step back on that matter in the near future. Recent events in the world influenced the way policy makers think about content regulations. 'The recent democratic movements in the Middle East and North Africa that started with the 'Green Movement' of Iran in the aftermath of the controversial 2009 presidential election to the 'Jasmine Revolution' in Tunisia which initiated many other waves of street protests in the Arab world, particularly in Egypt, Algeria and Libya, social media proved to be extremely powerful in mobilizing massive amount of people.' (Shirazi, 2012:920) Also London riots highlighted that the ability to communicate people, who may not even know each other, quickly and easily can lead to unimaginable consequences. Therefore extreme censors might have classified the social media as a more delicate issue than before and presumably justify their actions referring to those occurrences.

In the following section, online regulations in some countries including Australia, China, France, Germany, Iran, United Kingdom, United States of America will be discussed in detail in order to prepare a censorship report. Those countries are chosen deliberately. Every one of them has important characteristics regardless of whether positive or not. Along with the academic debate following this chapter, highlighting certain points of the regulations and jurisprudences in those countries will help us answer the main question of this research, which is how Turkey should proceed with the Internet regulations? The trajectory of the content regulations in Turkey will not be discussed in this chapter because it will be given in a separate one entitled Analysis of Online Content Regulations in Turkey which will be one of the milestones of this research. Turkey's position in censorship scale will be given at the end.

Here it should be noted that countries which will be studied below are not sorted from the best practices to the worst.

2.2 Country Evaluations

2.2.1 United States of America

The main purpose of this chapter is to show that free speech is not an obstacle in front of the online regulations. United States of America is the best example for this argument, because the country has a high codification level of human rights. This does not suggest that the country is the most successful at delivering the fundamental rights to everyone at every level. However the country's attempts to *maintain the balance* between the fundamental rights and protection of actors deserve particular attention. That is why firstly the scope of the First Amendment will be studied. After that several acts will be investigated in order to evaluate the consistency of the attempts with the constitution. Lastly findings of the chapter will be given.

United States of America's position in online content regulations is one of the strongest examples in the world regarding to the First Amendment of the Constitution, which guarantees a number of different rights. Freedom of religion, speech, the press, peaceably assembly and right to petition Government are all protected with the following statement:

> *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.*

Not surprisingly those rights extent to the Internet, too. Although government is trying to keep online regulations at minimum level, it did not prevent the country from having one of the most sophisticated content regulations, because the extension of the free speech is still one of the hottest debates. Public dialogue and legislative debates are far from reaching a political consensus on the best ways of protecting children and policing the offensive activities on the Internet.

The first endeavour to regulate indecency and obscenity on the Internet happened in 1996 with the Communications Decency Act. The CDA was a serious attempt, as it suggested 'transmitting 'indecent' or 'patently offensive' online content to recipients under eighteen years of age could result in a fine or imprisonment. However the Supreme Court decided that the terms 'indecent' and 'patently offensive' were left ambiguous and the act breached the freedom of speech principles. It was stated in the court decision that 'although the Government has an interest in protecting children from potentially harmful materials, the CDA pursues that interest by suppressing a large amount of speech that adults have a constitutional right to send and receive.' (Lievens, 2007:321) In 1998 another act called Child Online Protection Act, which criminalizes the communication of content, harmful to minors, for commercial purposes, except when access by minors had been restricted through verification of the Internet user's identity by requiring a credit card number, digital age certificate or by any reasonable measures feasible under available technology, roughly met with the same fate. (Lievens, 2007:321) Those were not the last attempts in the USA. Digital Millennium Copyright Act, Children's Online Privacy Protection Act and Children's Internet Protection Act were signed into law. Regardless from how successful and effective they are, those legislations indicate three important characteristics of the USA government's perspective on the Internet regulations. Firstly *the choice of legislation as the regulatory tool* to combat all Internet torts is the most plausible. The second characteristic lies under the efforts to *maintain the balance* among the fundamental rights, protection of actors and commercial and national interests. Furthermore, considering the scope of the legislations which have been brought into effect so far, the third characteristic highlights the main concerns of the Government, which are the protection of children, infringement of intellectual property rights and national security. The scope of online regulations in the United States of America seems reasonable.

On the other hand, it would be an optimistic view to say that the USA has found the best legal and technical means of protecting minors and IPR, and policing illegal activities. Tackling problematic content is a delicate, difficult (if not impossible) issue and may have serious collateral damages. Most of the time, according to the amount of the Internet traffic being monitored, it is too much expensive, as it requires heavy investments in human and technical resources. Besides, considering that maintaining such systems enables surveillance of all information running through them, it has the potential of violating the First Amendment. For that reason, Internet Service and Content Providers in the USA have been made *not liable* over the content, if they remove the objectionable content as soon as possible upon notification. However the legislations such as Stop Online Piracy Act (SOPA), which was rejected in its initial hearing and galvanized a massive response including a blackout by a number of service providers including Wikipedia, and Protect IP Act which were advertised as 'promoting prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property and for other purposes' put service providers, search engines, other Internet companies under burden of monitoring the Internet traffic in order to detect illegal content. Otherwise they might risk legal action, because private companies are allowed to sue those service providers for even briefly and unknowingly hosting infringing content.

To conclude, dialogues on American way of online regulations are expectedly still going on and the country is far from reaching a political and social consensus. Regardless of the current discussions on online copyright acts, according to the characteristics of legal framework mentioned above, the USA can be categorized as a moderate censor.

2.2.2 The United Kingdom

In this chapter, United Kingdom's online regulations will be studied. Firstly the Internet Watch Foundation's works will be given along with the liabilities of Internet Service Providers. Before sharing the findings of this chapter, some characteristics of country's regulations will be criticised.

The United Kingdom embraces a co-regulatory framework in which Intemet Service Providers, mobile network operators, government agencies and the police play important roles. Most of the literature introduces the Intemet Watch Foundation (IWF) as one of the most important component of this framework. The IWF, which was established in 1996 as an industry based self regulatory body, maintains and updates a blacklist of criminally offensive web pages including 'child abuse images and content that is criminally obscene or incites racial hatred.' (Deibert et al., 2008:188) As one of the earliest examples of the Internet hotlines, IWF is financed by the ISPs and supported by the UK Government. Its main task is to receive reports from the public, evaluate the illegality of the material and share it with the member ISPs. This task provoked the discussions about the validity of IWF's actions, because many academics underline that 'illegality should be a matter to be decided by courts of law and not by private organizations or by quasi-regulatory bodies and the industry proposals which advocate that the task of evaluating the legality or illegality of specific data is difficult for Internet providers and should, therefore, be integrated into the work of hotlines is wrong in principle and would be unacceptable in democratic societies.' (Akdeniz, 2001:307) On the other hand, considering that Internet hotlines are supported by the European Union's Action Plan for assisting ISPs and law enforcement agencies in various countries, this debate is far from reaching a closure. The IWFs efforts can be considered plausible, if the extension of its blacklist remains within the boundaries of commonly agreed Internet offenses.

Before explaining what happens after the IWF sends the blacklists to member ISPs, it would be better to introduce another important component of British content blocking system. In 2003, the largest ISP in the UK, British Telecom serving about a third of home Internet users, decided to create a comprehensive content blocking system called BT Anti-Child Abuse Initiative also known as CleanFeed. The project was launched in 2004 in consultation with the British Home Office. The first aim of this project was to filter the Internet content based on the IWF's blacklist of websites hosted outside of the country, that contain images of child abuse as defined by the amended Protection of Children Act, 1978. (Clayton, 2005:117, Deibert et al., 2008:188) Given that the extension of the project was broadened to filter websites which breach IPRs, the official name can be misleading.

Although the details of Cleanfeed are not officially shared with the public, the blocking process is considered to be running roughly as follows. First of all, HTTP requests to the foreign websites, whose one or more pages were classified as illegal by the IWF, are redirected to the proxy servers. If the requested URL is in the blacklist, user sees an error message as if the particular page is unavailable as a result of connectivity problems. Otherwise the traffic is forwarded through the server without being processed. Although the system is unfairly criticised as being similar to China's Great Firewall, it deserves credit as it blocks only the unwanted content rather than blocking the whole website. Considering the great diversity and brilliant features that Web 2.0 brought to the Internet, shutting down the whole platform just because of an unfortunate material does not follow the proportionality principle. For example, blocking Youtube because of one offensive video would affect millions of Internet users. On the other hand, illegal content that is hosted within the country is required to be taken down by ISPs and other content providers under a notice and take down regime. (Deibert et al., 2008:188)

The term voluntary is used in an unusual way in the UK, because all broadband consumer ISPs in the country are expected to have implemented a filtering system. Those failing to do so might face regulatory enforcements. Although the Government's position to mandate *voluntarily* use of URL filtering tools to all ISPs in the country is highly criticised, given that the consequences of online offenses might be catastrophic, this policy seems reasonable. However, for the possible misuse or abuse of such systems, ISPs and other service providers should be made accountable with clearly defined rules, which take into account of the Internet users' rights. Moreover, the IWF is not an accountable boy and its transparency is another issue. Some academics state that 'the absence of openness, and transparency of the work of the hotlines as well as the secrecy surrounding the blocking criteria and the list of blocked websites, concerns will continue to exist about the work of such organizations.' (Akdeniz, 2010:266) If British policy makers clarify those issues, this might help eliminate public concerns about the protection of individual rights and increase public support.

To summarize, the recent legislations do not alarm the blocking of religious and political content over the Internet, the UK can also be classified as moderate censor as well. Ambiguity of the CleanFeed structure which was highlighted above is the most noteworthy point in the country's online regulations.

2.2.3 France

In this chapter, firstly some political aspects and the scope of France's regulations will be given. After that HADOPI Law will be discussed as it attracted serious attention from all over the world. Lastly some critics about this law and country's position in censorship scale will be given.

France's internet regulation scheme is one of the most controversial ones in Europe. The Government embraces a content blocking system based on black lists maintained by the Ministry of the Interior. Those blacklists contain websites which promote child pornography, infringement of IPR, terrorism, racial violence and hatred. France is one those countries where hate speech is addressed the most vigorously in Europe. Therefore the country has a minimum tolerance against such online content. Apart from those mentioned above, websites which deny the Holocaust and promote Nazism are blocked in France at ISP level. (Deibert et al., 2008:154) This can be considered as an example of website blocking based on political reasons.

The latest law called HADOPI (Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet) highlights the latest concern of the Government. With this law, French Government intends to promote the transmission and protection of creative works on the Internet by preventing the downloads and shares of the copyrighted material without the consent of the owner.

HADOPI is an acronym which represents the High Authority for Transmission of Creative Works and Copyright Protection on the Internet. The authority, which consists of 9 members from judicial, legislative bodies and other government agencies, is empowered to police Internet users in order to eliminate the infringement of IPR. Having representatives from different bodies can be considered as a sign of Government's good will on content filtering, but because of several reasons which will be given below it is difficult to claim that it has been widely supported.

The procedure of the law is as follows. If the authority receives a complaint from a copyright owner or their representatives about an Internet user accused of infringing the copyright and that is supported with evidence, a three strike process is initiated. Firstly, the subscriber is sent an email message saying that he has been breaching the law and should stop doing it and secure his internet connection in case of someone else is maliciously exploiting his resources. From that moment, subscriber's internet traffic is monitored by the ISP. Here two issues have to be underlined. Every ISP has to install a traffic surveillance system and online activities of suspected users are monitored upon copyright infringement accusations. This is one of the points for which HADOPI is severely criticised, as the Government is accused of violating personal privacy.

Despite the email notification, if the subscriber repeats the infringement within the first six months and this is reported by ISPs, copyright holder or representatives to the authority, the second stage of the three strike process begins. HADOPI sends a similar message to the subscriber via a certified letter informing that if the offense is repeated within the following year the user can face serious consequences such as the suspension or cancellation of the Internet service or even prosecution. The last step occurs if the user persists on repeating the offense. The authority might order the ISP to suspend the internet service of the subscriber from a period that may range from two months to one year. That penalty flamed another debate. In his report, entitled The Promotion and Protection of The Right to Freedom of Opinion and Expression, the United Nations' Special rapporteur Frank La Rue, stressed that cutting off users from Internet access, regardless of the justification provided, is disproportionate and thus a violation of civil and political rights. (Rue, 2009:21)

To conclude, three-strike model requires certain level of computer literacy and suggests that subscribers should be able to adequately secure their wireless internet connection or install and operate the necessary software in order to prevent from being involved in offending activities. This suggestion is the bottleneck of the HADOPI legislations. Because of that reason along with other filtering cases based upon political reasons, France is on the edge of extremism and can be classified as a *more than moderate* censor.

2.2.4 Germany

The outset of this chapter is as follows. Firstly the affects of the German Criminal Code on online regulations will be studied. After some important actors of the Internet introduced, examples of website blocking will be given in order to analyse country's regulatory framework better. Lastly the chapter will be concluded with the findings.

The scope of illegal content that is filtered in Germany is generally limited to distribution of pornography to minors, racism and material that promotes infringement of IPR, hatred and terrorism, as it is the case almost in every country in Europe. The Government mainly concerns about two topics, which are the protection of youth from harmful material such as pornography and incitement to hate or violence against a group of people. Regulations about those issues are based on laws. This is one of the plausible characteristic of German regulations. In Germany, filtering at source is embraced as a regulation mentality and this take various forms when it comes to the Internet regulations. Examples of this argument will be given further.

First of all, the German Criminal Code states that ''whoever, in relation to pornographic writings, offers, gives or makes them accessible to a person under eighteen years of age shall be punished with imprisonment for not more than one year or a fine.' For that reason, the dissemination of pornographic performances through Internet is prohibited if the provider does not ensure that the performance is not accessible to minors less than eighteen years of age by technical or other means. Specifically, the Youth Media Protection Treaty regulates the electronic media including the Internet for the protection of minors. These laws are taken as a requirement for web sites with adult content to implement a strict age verification system. Those which fail to comply with those requirements are blocked by ISPs. Actually, Germany can be considered as a successful example which managed to impose its Internet regulatory framework to foreign websites as well. Flickr is the most famous example for this argument. In its 'content filters' web page Flickr announces that if the Internet user's login credentials are based in Germany, he will not be able to view the restricted content due to local terms of service. Whether this methodology is successful or not is debatable, but this situation reflects the influences of German laws on cyberspace.

In 2009 the Government signed *voluntary* contracts with major ISPs through The German Federal Criminal Police and The Ministry of Family Affairs in order to find an effective way for combating child pornography. According to the contacts, all ISPs must block the pornographic websites included in the blacklists which were provided by The German Federal Criminal Office. (Deibert et al., 2010:310) The content of the blacklist is not open to the public. When Internet users want to access to those pages, they will see a warning page indicating that the content is illegal. The requests are redirected to those warning pages through DNS manipulations. As long as the extent of blacklists remains within the boundaries of crimes which were clearly identified in the law such as child pornography, this kind of filtering concerns can be considered as reasonable. However the effectiveness of DNS filtering is another issue, as it remains a clumsy technique compared to the advanced features of circumvention tools.

Unlike the UK, in Germany, classification of content which is considered to be harmful to children is classified by a government agency called the Federal Department for Media

Harmful to Young Persons, which traditionally censors films, print media and computer games, but has expanded its focus to the Internet, too. The authority prepares blacklists of websites which broadcast harmful content to minors in order to make them inaccessible within the country. Since 2005, the authority maintained strong relationships with major search engines including Google, Lycos, AOL and Yahoo. According to the blacklists, local versions of those search engines filter their search results. Therefore content filtering occurs in search engines as well. The details of those blacklists are not shared with public in order to avoid pressure. Search engines are not allowed to disclose them, either. This issue is expectedly highly criticized due to transparency concerns.

Moreover, like France, Germany's legislations involve some political aspects based on the German Criminal Law. The Public Incitement Law, which was lastly revised in 2005, states that 'whoever, in a manner that is capable of disturbing the public peace, incites hatred against segments of the population or calls for violent or arbitrary measures against them; or assaults the human dignity of others by insulting, maliciously maligning, or defaming segments of the population, shall be punished with imprisonment from three months to five years.' Reflection of this law in the cyberspace is blocking the offensive material. In Germany, it is forbidden to publish right wing propaganda such as denying holocaust on websites and those which contradict with the law are blocked. Moreover notice and take down procedures are followed, too. For example, as it was given before, websites containing Nazi propaganda are deemed illegal and blocked at ISP level. There might be found other examples, but 'the most prominent example is YouTube. In August 2007, German politicians and the Central Council of Jews in Germany complained about the extremist content that was being hosted on YouTube. The company removed the illegal content from its website upon notification and a spokesman promptly promised to improve the system of takedowns to comply with the demands of German law.' (Deibert et al., 2010:310)

In conclusion, Germany's position in Censorship scale is a controversial one. Country chooses legislations as regulatory tools, but the extension of content filtering expands to political areas and, as in the Flickr case, sometimes violates constitutional rights of adults. On the other hand, restrictions are not as strict as those in France. For that reason, Germany can be classified as a moderate censor.

From this point forward, there will be no more European countries investigated. However, some examples might be given according to the context. After studying Australian regulations in the next chapter, the most restrictive regimes will be analysed.

2.2.5 Australia

Australia's regulatory framework is a good case which deserves deeper analysis. Firstly the country's regulatory body and its works will be given. The main purpose of this chapter is to introduce the online classification system. After analysing the procedures and several characteristics, findings of this chapter will be presented.

Australia is one of the most interesting cases which have different characteristics, although it follows the footsteps of developed western countries. The literature about the Australian regulation scheme firstly underlines the fact that 'Australia's constitution does not explicitly give the right to free speech and in fact contains a clause giving Australian government communication power, allowing it regulate postal, telegraphic, telephonic and other like services including the Internet.' (Deibert et al., 2010:391, Armstrong, 2002:231) Because of that reason different legislations occur in different states.

Australian Internet content regulation scheme was based on the Broadcasting Services Act 1992 which gave the broadcasters 'the primary responsibility for managing content by means of codes of practice detailing the level of material that may be broadcasted within a framework of rules and reserve regulatory powers' (Lievens, 2007:323)

The Australian Media and Communication Authority (ACMA) is the regulatory government agency which ensures illegal content not accessible to Australian citizens. ACMA basically has four responsibilities, which are receiving complaints from the Internet users, following notice-take down procedures, certifying web filter manufacturers and developing necessary regulations. The authority is not mandated to monitor the Internet traffic to find out the prohibited content, but it is allowed to begin investigations without an outside complaint. The scope of web pages that might be subject to notice and takedown procedures is defined under the Commonwealth Classification Act 1995. Web content which falls under any of those categories might be prohibited.

1. R18: Contains material that is likely to be disturbing to those under 18. This content is not prohibited on domestic hosting sites *if there is an age verification system certified by the ACMA* in place.

This suggestion is both plausible and dangerous depending on which technology is chosen for age verification. First of all, those attempts rise from the righteous concern that blocking particular content because of the necessity to protect minors has potential to violate the rights of adults and another way should be found to compromise. Because of that reason, although many people resist, age verification technologies are addressed in many debates. Obviously Australian authorities embrace such technologies, too. However, early applications such as providing a welcome page with a warning saying that 'this platform contains explicit material and might be harmful to minors' are not fruitful, as for children it is just a click away to reach the objectionable pages. On the other hand, using age verification technologies based on credit cards or independently issued identities have other bottlenecks. For example, people might not want to give their personal details due to privacy and security concerns. Even if they agreed to do so, children might have access to those credentials as well. Moreover how this system will apply to overseas websites, newsgroups and chat is ambiguous.

'When people fall into the trap of believing or, more accurately, hoping that technology will solve the problems, they are actually abdicating the high touch of personal responsibility.' (Naisbitt, 1982:53) Even if an effective methodology is found for age verification, policies which are mainly based on those systems will be weak and can simply be a part of the solution.

2. X18: Contains nonviolent sexually explicit content between consenting adults. This content may be subject to ACMA takedown provisions if hosted on domestic servers.

3. RC: Contains content which is 'Refused Classification' (child pornography, fetish, detailed instruction on crime such as bomb making) and is prohibited on Australian-hosted Web sites.

Once ACMA determines that a particular content, which is hosted within the country, should be prohibited, it issues a notice and take down notice to the Internet content providers. If the provider does not remove the content upon notification, it might face legal consequences. On the other hand, if the content is hosted in overseas servers, ACMA follows a different procedure. To articulate the procedure, additional information is necessary. In Australia Internet Service Providers are mandated to provide free family filters to their subscribers. Those filtering software are produced by certified manufacturers. Once a company is certified by ACMA, it has to download and update the blacklists from ACMA and upload those confidential lists to the clients who are using the filtering software of this particular company. The blacklists contain the offensive websites that are hosted in another country. Here it might be useful to state that home Internet users do not have to use those filters in their personal computers. That is why, not surprisingly offensive material remains accessible to many Australian citizens.

To overcome this issue, in December 2007, 'Telecommunications Minister Stephen Conroy announced a strengthened Cleanfeed policy, under which all Australian ISPs are required to provide Internet filtering services that prevent child pornography and other inappropriate material from reaching schools and houses.' (Deibert et al., 2010:394) ACMA has started trials with major ISPs for content filtering and published test results in its webpage. At the moment of speaking, this issue is not supported by the parliament. Also ACMA released a new regulatory framework in 2007, which requires all content service providers to implement age verification systems if their websites publish adult material. In the Australian Law Reform Commission's website, specifically in Restricting Access to Adult Content page, those attempts are mentioned as 'reasonable steps to restrict access.' Furthermore in 2008, 'the government announced plans for a layered filtering scheme, proposing a mandatory filter to block pornographic and illegal content, as well as an opt-out filter that would block even more content.' (Deibert et al., 2010:391)

As a conclusion, Australian regulations indicate that policy makers embrace a modular approach rather than a block solution. They are trying to include all actors of the online industry into the framework. Although many scholars and activists consider those efforts as signs of a restrictive regime, Australian authorities evidently do not intend to loosen the controls in the near future. Given that there is not enough evidence about Australia is violating human rights in the cyberspace, the country can be classified as a moderate censor.

2.2.6 The People's Republic of China

In this chapter, one of the most comprehensive filtering systems of the world will be given. Firstly concerns of the Communist Party and liabilities of different actors in online environment will be studied. Also responses of important companies to online regulations will be studied, before the chapter reaches conclusion with some important findings.

The People's Republic of China deserves a particular attention to its intemet regulations. It is a well-known fact that there is no other country which heavily invests and allocates resources in online censorship as much as China does. The government does not only filters objectionable content, but also monitors the intemet traffic in order to make sure online materials containing certain keywords do not flow to the individuals. All actors including ISPs, content providers, media, companies, internet cafes, search engines and even individuals are subject to a set of rules of a restrictive regime.

In the 1997 regulations entitled 'the Computer Information Network and Internet Security, Protection, and Management Regulations', it is stated that 'these regulations have been established in order to strengthen the security and the protection of computer information networks and of the Internet, and to preserve the social order and social stability.' But when recent controls and consequences are considered, the regulations not surprisingly were put into effect to protect the Communist Party's ideological and political dominance by preventing the use of media in an 'unhealthy way'. (Tan et al., 1997:12) Chinese government considers the exposure to the materials created by opponents of the government and foreign countries, which have different political, cultural and economic structures, as a serious threat to the regime. The Government is also aware of the fact that the more communication networks develop and provide new opportunities, the more organizations and individuals are capable of collecting, processing and distributing the kind of information which used to provide China's central government with the power to maintain its controlling position. That is why the regulations and filtering techniques are becoming more sophisticated every day.

The 1997 Regulations contain serious sanctions to the actors of the Internet industry. All ISPs and other commercial service providers are mandated to comply with the rules and guidance of the Public Security Bureau whose primary responsibility was defined as 'maintaining the network security.' ISPs and other commercial service providers have to assist the PSB with the inspection of criminal activities and prepare reports about the demographics of the Internet usage and make sure the traffic flowing through their infrastructure *obeys the rules*. This requires investment in filtering and traffic monitoring systems. Any violation might end up with the cancellation of business licence, prosecution and arrestment of the company staff and the user involved in criminal or harmful activities. The details of such activities are as follows.

Users are not allowed to create, acquire or distribute any kind of information which:

1. Incites to resist or breaking the Constitution or laws or the implementation of administrative regulations;
1. Incites to overthrow the government or the socialist system;
2. Incites division of the country, harming national unification;
3. Incites hatred or discrimination among nationalities or harming the unity of the nationalities;
4. Makes falsehoods or distorting the truth, spreading rumours, destroying the order of society;
5. Promotes feudal superstitions, sexually suggestive material, gambling, violence, murder;
6. Promotes terrorism or incites others to criminal activity; openly insults other people or distorts the truth to slander people;
7. Injures the reputation of state organizations;
8. Involves other activities against the Constitution, laws or administrative regulations.

Those rules are too broad and contain many uncertainties. As introduced before, such uncertainties create a 'panopticon effect' and eventually trigger self-censorship policies. Companies, content providers and even individuals censor their own communications in order to avoid legal consequences. This actually helps the Communist Party keep things under control, as they know it is impossible to monitor every material, and people will always find ways around no matter how advanced and extensive the filtering solutions are.

The extension of Internet regulations in China is so broad that Government obviously does not want to leave any channel unattended. Web users in Internet cafes must provide personal information to be able to go online and the rules given above apply to such public places as well. In addition, with the introduction of the Golden Shield Project in 2006, it is estimated that around 50.000 police officers have been employed to scan blogs, discussion forums and other websites to ensure the contents do not challenge the interests of the Government.

Additionally, according to the Measures on Internet Information Services Article 9, profit making companies seeking to operate bulletin boards or other electronic communication services were required to obtain approval from the Ministry of Information Industry and other websites can only publish what licensed companies already broadcasted. Linking to overseas news websites is prohibited and content providers are responsible for ensuring the legality of any information disseminated thorough their services. Therefore they were charged with monitoring all content on their services and immediately removing and reporting any inappropriate or illegal postings.

Furthermore, search engines suffer from a different dilemma. Although they do not want to contradict to their own policies about free flow of information and human rights, given that China has the most crowded population of Internet users, and therefore it is a fruitful market for commercial enterprises, search engines do not want to stop their operations in the mainland. Eventually many search engines created a local version and started to censor the search results in compliance with the Chinese laws and regulations. For example, after a long time of tension with the Government, Google agreed to filter search results and started to show a warning page to the users who make searches about sensitive words referring to Tiananmen Square incidents, Dalai Lama, pornography etc. When a user searches for 'anti communist', he faces a warning page saying that 'We have observed that searching for 'anti communist' in mainland China may temporarily break your connection to Google. This interruption is outside Google's control.'

Another important point of Chinese Internet regulations is the fact that there are twelve government agencies involved in those efforts. Central Propaganda Department, Department of Commerce, Department of Telecommunications, General Administration of Press and Publications, Ministry of Culture, Ministry of Information Industry, Ministry of Public Security, Public Security Bureau, State Administration of Radio Film and Television, State

Council, State Council Information Agency and lastly State Secrets Bureau might individually intervene to the operations of Internet actors within the country. This makes the situation even more complicated, as the number of topics which companies or users should concern about is substantially higher compared to any other country.

In conclusion, the most critical point of Internet regulations in China is the *uncertainty*. The list of the prohibited web sites is not public and there is no way to question the underlying reasons. Definitions in the legislations are nonspecific and broad. The authorities are unsurprisingly not accountable for their actions. Therefore regulations seriously lack transparency. As a result, citizens do not want to risk themselves by testing the boundaries of the sensitive areas.

The issues such as infringement of IPR, parental control, network neutrality are deliberately not discussed within the context of Chinese legal code, because the country suffers from more fundamental challenges. To come to a conclusion, considering the issues discussed above, the People's Republic of China is classified as an extreme censor.

2.2.7 The Islamic Republic of Iran

In this chapter, after introducing the constitutional statement of the Islamic Republic of Iran regarding to media regulations, liabilities of several actors will be studied. After that the government's R&D efforts to fix the bottlenecks of the Internet which is considered a threat to the regime, as it relies on Western technologies will be given. Moreover responses of Internet users to circumvent filtering and government's efforts in response to circumvention will be other important points of this chapter. Lastly the findings of Iranian online regulations will be given.

Islamic Republic of Iran is one of those countries which consider the increasing popularity of the Internet a threat to the regime. The government deems the Internet just another form of mass communication media such as radio and television. Therefore there has been an attempt to apply the same regulations and legislations to the online world, too.

According to the constitution which was last amended in 1989:

> *The mass communication media, radio and television, must serve the diffusion of Islamic culture in pursuit of the evolutionary course of the Islamic Revolution. To this*

> *end, the media should be used as a forum for healthy encounter of different ideas, but they must strictly refrain from diffusion and propagation of destructive and anti-Islamic practices. (Farivar, 2011:166)*

As in the case of China, the same uncertainties and broad definitions exist in the constitution of Islamic Republic of Iran. The ambiguous terms 'healthy' and 'destructive practices' are two bottlenecks of the regulations which are quite strict in the country. Details are given below.

First of all, all ISPs in Iran are mandated to install a filtering system 'to block different types of online dialogue from carrying political and religious conversations, divergent views and discussions related to women's rights, and to sites hosting pornography or gambling activities.' (Shirazi, 2012:923) According to the author of the cited paper, who is an Iranian researcher at the Ryerson University in Canada, the Government employs all kinds of filtering techniques such as IP blocking, DNS manipulation and deep packet inspection. Shirazi also states that DNS filtering is mostly used for filtering the web sites of opposition groups, sites related to ethnic and religious minorities as well as sites that are deemed to be 'immoral'. (Shirazi, 2012:923) Not surprisingly the blacklists of those domains are not disclosed by the authorities and the boundaries of the *immorality* are ambiguous. IP filtering, which makes numerous websites which are hosted in the same server inaccessible to the users in Iran, is mostly preferred to block foreign websites. Lastly the Government favours the deep packet inspection technologies which examine all kinds of content flowing through the gateways for specific keywords. Social networking platforms such as Facebook and Twitter, blogs, emails are all monitored and ISPs report the activities, which are deemed to violate the country's laws and regulations or if the activities indicate criticism against the elites. (Shirazi, 2012:923)

Shirazi states that Nokia-Siemens or Secure Computing, which was acquired by McAfee, is helping the Iranian authorities to intercept the data network within the country. (Shirazi, 2012:923) Regardless of the nationality of the deep packet inspection solutions, the Government does not want to be dependent to foreign technologies, because 'the reliance on western technologies is seen as a source of weakness and a potential vulnerability for the integrity of the Iranian Internet.' Also authorities are concerned 'that Western software might include a 'backdoor' that would give outsiders access to key infrastructure.' (Deibert et al., 2010:549) Given the cyber-attacks on the country via the Stuxnet worm which destroyed hundreds of uranium enrichment centrifuges in Iran's Natanz facility, those attempts seems reasonable. For this purpose, inevitably research and development of domestic products has been financed by the Government. Those R&D efforts will certainly contribute to the country's competency in information and communication technologies and might seem plausible. However the motive behind those actions is alarming and suggests a more isolated and suppressed Internet in the future.

In addition, according to a report on the Status of the Internet in Iran, which was prepared by Iran's Civil Society Organizations Training and Research Centre (ICTRC), 'the government does not approve the use of high speed Internet by the public, because according to the Constitution, the Islamic Republic of Iran's Broadcasting has monopoly on radio and television broadcasting; a monopoly which will be jeopardized if people could have access to radio and TV programs online using high speed Internet connection.' Therefore, high speed internet access is only available to government agencies and a handful registered firms. (Shirazi, 2012:921) To verify this claim, a small speed test might help. According to the test results generated by Net Index website, users in Iran are experiencing almost the slowest Internet speed in the world. This regulation is obviously based on the argument that citizens are not capable of distinguishing the harmful (or illegal) and appropriate content, if not all citizens are considered to be potential outlaws by the authorities.

Along with the slow download rates, this situation has another bottleneck. Under the microscope of authorities, many Internet users in Iran used to enjoy web proxies or virtual private networks to reach outside world and communicate with people in other countries. According to Pakistan's most widely read English-language newspaper, Dawn, the head of the specialised police unit of Iran stated that 'about 20 to 30 percent of Iranian Internet users use VPN'. Since such technologies place a heavy load on the Internet connection due to encryption of the payload, users experienced substantial delays in data transfer and eventually become discouraged from using them. This issue is much more problematic when it comes to download large files such as video and music.

Furthermore, Iran is one of the most dynamic countries in terms of the number of web bloggers and, along with other media sources they are also subject to the regulatory authority of the Press Supervisory Board under the Ministry of Islamic Culture and Guidance. (Deibert, 2010:550; Shirazi, 2012:924) In the same ICTRC report, it is stated that 'the biggest Iranian weblog service provider, PersianBlog, included in its terms of agreement that bloggers must observe ethical principles, country's laws, and avoid publishing material jeopardizing the national independence and security.' Again the terms 'ethical principles' and 'issues jeopardizing national independence and security' are broad and uncertain. There is no authority in Iran for determining the boundaries of those issues. Therefore bloggers are discouraged from pushing the limits and weblog service providers apply strict terms of agreement to avoid legal consequences. It is worth considering that there are many cases in Iran regarding to imprisonment of bloggers. In 2003, Sina Motalebi was arrested because of his writings in his blog and his interviews with foreign media and this case was the beginning of a period of arrest and imprisonment of bloggers. According to the report submitted by Human Rights Watch (HRW) to the UN Human Rights Committee:

> *A former judge Saeed Mortazavi who is known for ordering the closure of numerous reformist publications in the early 2000s organized the arbitrary detention of more than 20 bloggers and journalists in 2004 and held them in secret prisons, where security forces compelled them to make false confessions. In 2010, a Revolutionary Court sentenced a prominent Iranian blogger Hossein Derakhshan to 19 and half years in prison, which is criticized to be the heaviest sentence against a blogger so far. (HRW, 2011:11)*

Lastly, owners of Internet cafes are mandated to install cameras in their facilities and maintain the web browsing history and camera records of their customers. Those records must be kept for six months and must be given to the police if asked. Also users are required to provide an identity card when visiting the Internet cafes in the country. Besides full name, name of the father, national identification number, address and telephone number of each customer must be written down, so that police can track down those users in case of illegal occurrences.

In conclusion, in the Islamic Republic of Iran people with different political and religious views are considered to be threat to the regime. The government is intimidated by the power of online communications so much that it is reported that 'the authorities unplugged the entire network in Iran during the 2009 political turbulences.' (Shirazi, 2012:925) In a country where fundamental rights are problematic and violated by the authorities, legislations such as infringement of IPR and parental control remain collateral. Because of this reason those issues were not studied in Iran's case. Considering all the factors given above, the Islamic Republic of Iran can be classified as an extreme censor.

2.3 Last Words on Censorship

The countries studied above are chosen carefully as important and diverse representatives of dominant perspectives on Internet regulations. There is no country in the world in which authorities do not intervene in online activities. Even the authorities in New Zealand, which remained silent about Internet regulations for a long time and meanwhile carefully observed what the others did, have started to talk about following footsteps of one or several different best practise models. Findings of an interesting research project about online behaviours conducted in New Zealand will be given further.

As it can be clearly seen from the examples above, the extent of government interventions in online activities relies upon many factors such as the political structure, legal framework, social concerns and interests of many different actors. Authorities ask different questions, surely reach various conclusions and eventually come up with different policies. On the other hand, it should be noted that there are similarities between the extremists and moderate censors, too. Although those similarities remain minors compared to the differences, they are worth noting.

First of all, governments consider ISPs important actors and place liabilities on them. Whether voluntary or mandatory, ISPs have to implement IP logging or content filtering systems. In the UK, ISPs are required to maintain logs of IP addresses assigned to customers in some cases, whereas in Iran and China ISPs have to implement comprehensive monitoring systems with deep packet inspection capabilities. Secondly, in every country including those discussed above, ISPs have to assist law enforcement agencies when requested.

Moreover, almost every country uses legislation as the regulatory tool. It is evident from the examples that this is only plausible if harmful and illegal activities are defined clearly in the regulations, after the fundamental human rights are protected by laws. Uncertainty leads to censorship policies. When content providers and Internet users do not know the boundaries of sensitive areas, they fall apart from the fruitful experiences that Internet offers. If people are intimidated because of the uncertainty, they might not share or view even useful contents in order to avoid legal consequences.

Another similarity is a social issue. There is no country in which non-governmental organizations, politicians and authorities are entirely in agreement about the necessity of censorship policies. For example, even when a website is filtered due to its provision of bomb making instructions or a dangerous content which is doubtlessly a threat to national security, rivals argue that Internet is the reflection of the real life and it should be up to people to decide whether something is right or wrong. On the other hand, governments respond to such content providers with low tolerance. Considering that dependency on information and communication technologies increases every day, threats are expected to become more serious. This argument suggests that regulations will not be loosened in the future. Therefore censorship debate is far from reaching a conclusion.

The only matter on which there is a common agreement is the protection of minors. Although academics, politicians and all related actors suggest that child pornography, online abuse of children and dissemination of pornography to minors should be given the first priority; there is no single solution on which they come to an agreement. Developed countries such as Australia, the United States of America and major European countries, deal with this issue by taking different precautions. Age verification systems, parental control or simply maintaining blacklists of harmful websites and making them inaccessible to users within the country are some of the measures. In some countries in the Middle East and North Africa region and East Asia, not only child pornography but also other kinds of obscenity are deemed harmful and blocked. Given that there is a huge pornography sector involving global companies in media and entertainment such as AOL Time Warner Inc (Haney, 2006:49), it is sensible that the governments want to protect the interests of such companies by loosening the regulations on this matter. However in numerous countries, due to various reasons, regulations about pornography are quite strict. In the following chapter, different opinions on this issue will be studied.

Differences in the Internet regulations sometimes occur due to the different interpretations of the same problem, but the way authorities make decisions always relies upon the *needs and constraints*. When France is considered, the country introduced the most controversial Internet regulation in its history, HADOPI, in order to *solve* one of the major challenges of the online world. Due to the substantial increase in the infringement of intellectual property rights, which will be another pillar of the following section, policy makers risked the country's reputation by introducing three strike procedures which have the potential of violating individuals' rights in various ways. This regulation clearly suggests that in France, the needs of the industry come before individuals' rights to communicate with others. On the other hand, HADOPI highlights the fact that infringement of IPR on the Internet has become a destructive problem for the people involved in the creative works. Because of that, this problem deserves a particular attention and will be investigated from an academic perspective in the following chapter. Moreover why other developed countries are not making such strict regulations to combat this tort is a good question and the answer points out another important issue.

To conclude, in most of the developed countries especially in the United States of America, freedom of speech is highly embraced and protected by the constitutions or laws as in the case of the United Kingdom which does not have a constitution. Therefore Intemet issues are evaluated under the context of fundamental human rights. This is a valuable lesson which should be studied in depth and applied not only to the Internet but also other areas. However, considering the serious consequences of the Internet torts, boundaries of the right to free speech become the main concern. Authorities have never been so challenged to observe the balance between fundamental human rights and national and social interests. Because of that reason in the following section, this topic will studied in depth.

3. THE DEBATE

As it can be clearly seen from the previous chapters, there are three main issues regarding to Internet regulations. The first part of this chapter covers the first controversial issue, Freedom of Expression. After that Infringement of Intellectual Property Rights which is also a hot issue worldwide will be investigated. Pornography, obscenity and parental control are the main issues of the last part of this chapter.

3.1 Freedom of Expression

Freedom of expression is a fundamental human right to express one's ideas and opinions freely through speech, writing and other means of communication without governmental or third party interference. It is considered to be the most important milestone to safeguard democracy, because without it individuals cannot vote or take part in more informed public decision making. 'The right to express oneself enables an open debate about political, social and moral values, and encourages artistic and scholarly endeavour free of inhibitions.' (Jacobs and White, 1996:223) Violations of this important right may lead to undesirable consequences. Because of that reason governments and regional organizations have made admirable efforts recently in terms of securing respect for the right to freedom of expression. For example, the Universal Declaration on Human Rights Article 19, the International Covenant on Civil and Political Rights Article 19, the American Convention on Human Rights Article 13, The African Charter on Human and Peoples Rights Article 9, and the European Convention for the Protection of Human Rights and Fundamental Freedoms Article 10 are all important grounds for it. (Jorgensen, 2001:33)

Not all of those articles will be investigated, but highlighting at least two of them might be of use.

Article 19 of the International Covenant on Civil and Political Rights states that:

> *Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. The exercise of the rights carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary; for respect of the rights or reputations of others and for the protection of national security or of public order, or of public health and morals.*

The first part of the Article 19 draws attention to personal autonomy and presents a broad picture of freedom of expression, whereas the second paragraph clearly states that there can be limitations to this fundamental right. Almost the same approach exists in other declarations as well. Article 10 of the European Convention for the protection of Human Rights and Fundamental Freedoms states that:

> 1. *Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
>
> 2. *The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

The second paragraph clearly states that freedom of expression is not an absolute right and subject to some legitimate restrictions. Here it should be noted that what is legitimate is treated differently in different countries. Some countries may take a very expansive view of what is 'moral' or 'public health'.

Both of the articles above have two things in common. They clearly underline that such rights are independent from the nationality or social statue of individuals and suggest that governments should provide the necessary environments to protect them. The second point is the fact that even such freedoms have limitations. The main concem of this chapter is not questioning the legitimacy of such declarations. It is unquestionable that such rights are indispensable conditions for democracy. However the restrictions and conditions are important aspects for public order and protection of certain values. Because of that reason governments develop legal and regulatory frameworks for media activities, although much of which are criticized for being not fair and too much restrictive. Regardless of the faimess of such attempts, there is not a single country in the world in which radio, television, press and other means of communications are not subject to regulations. The question is where Internet should stand under such regulations? Considering that Internet has its own characteristics, should it be treated the same as other electronic media?

To clarify whether such restrictions apply to the Internet, the Committee of Ministers of the Council of Europe made a declaration which states:

> *freedom of expression, information and communication should be respected in a digital as well as in a non-digital environment, and should not be subject to restrictions other than those provided for in Article 10, simply because communication is carried in digital form. In guaranteeing freedom of expression, member states should ensure that national legislation to combat illegal content, for example racism, racial discrimination and child pornography, applies equally to offences committed via information and communication technologies. Member states should maintain and enhance legal and practical measures to prevent state and private censorship.*

There is a common agreement that 'applying guarantees under Article 10 to the digital universe does not appear to raise any obstacle of principle.' (Montero and Enis, 2011:23) However for some academics, considering that the Internet provides with more possibilities of a genuine public discussion space, it is more than the other electronic media and should not be treated the same in terms of drawing boundaries for the freedom of expression. It provides individuals what is essentially a new means of expressing themselves, seeking information, meeting, debating, and potentially opposing the system. (Jorgensen, 2001:42, Rowland and Macdonald, 2005:462) Also it is argued to be less invasive compared to radio or television based on the requirements to receive information on cyber space. An example might be useful to articulate the term 'invasiveness' of conventional media. Unless the broadcast is only accessible by providing some user credentials, when the radio and television broadcasts reach to the houses, everybody including children can stumble on the programmes by turning a dial. Therefore users might encounter unpleasant pictures and sound from television and radio, which enter the living room once the devices are turned on. This characteristic of such electronic media is frequently used to justify the censorship of obscenity or indecent speech.

There is an extensive literature which refers to the decisions of United States Supreme Court about the provisions of Communications Decency Act 1996 in order to compare Internet to mass media. (Price, 2002:163, Paul et al., 2004:307, Jorgensen, 2001:69, Rowland and Macdonald, 2005:462)

> *When assessing Internet as media the Supreme Court applied the notions of 'regulation history', of 'frequency scarcity' and of 'invasive nature', which were recognised as justifying regulation of the broadcast media. The Supreme Court*

> *agreed that these three factors were not present in cyberspace, and therefore previous broadcasting cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to Internet. (Jorgensen, 2001:69)*

The Court concluded 'the existence of warning screens and document descriptions dictates that the odds are slim that a user would enter a sexually explicit site by accident. Unlike radio and television, use of the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial.' Typing the domain name of the websites to the address bar or searching according to specific keywords in a search engine and choosing one of the results to click on are some examples of those affirmative steps. Moreover reaching to the materials in discussion groups and bulletin boards and joining a chat platform requires several more steps. Therefore it is argued that enforcing existing laws to the cyber space is not a fruitful approach.

This perspective contains a dangerous oversimplification by stating that 'the odds are slim that a user would enter a sexually explicit site by accident.' Internet has introduced various new communication channels which come with harmful potential providing accidental access to objectionable content. Pop-up adverts, junk e-mails, trojans, a back link placed within text in a page can easily direct people, including children, to unwanted materials. There are also other means available. According to a research called Internet Literacy Among Children and Young People conducted by London School of Economics and Political Science, children between 9 and 19 years old were asked about 15 risky activities and the results are as follows:

> *38% of children seen a pop-up advert for a pornographic site by accident, and 36% of which ended up on the sites which were advertised. 25% received a porn junk mail by e-mail. The same survey also reports that 22% of children ended up on a site showing violent images by accident and 9% encountered a racist website by accident. The report also notes that parents claim that their children have experienced substantially lower levels of online risk, possible because they are unaware of their children's activities or possibly because they define risk differently. (Livingstone et al., 2005:13)*

Pornographic and violent images are only the tip the iceberg. The same research also suggests that 70% of children would give out their personal information to win a prize online and 46% of them have given out their personal information to someone they met online. Also considering that the Internet has more powerful and diverse communication channels compared to the other electronic media and the communication does not necessarily have to be unidirectional as it is in radio and television; children are more vulnerable in the cyber space. Therefore limitations mentioned in the fundamental right declarations should also apply to the Internet, at least for the protection of minors.

Another issue is that the Internet is a global network of computers, servers, telecommunication paths and numerous devices without national boundaries. Anybody can gain access to this network anywhere without permission. Also there is not centralized storage location or control point. Therefore it is a decentralized and global medium of communication. Those features are some of the important characteristics of the Internet, but at the same time they frequently cause serious problems. Once something is shared online, in many cases it is almost impossible to remove it. This might not be a problem if the material shared online is an innocent family photo or a critique on the latest regulations of the government. However damaging somebody's reputation by publishing false and malicious statements on a national online bulletin or uploading a video showing how the soldiers were killed by terrorists are serious issues, especially when the content is followed by many people. Given that there are many ways to reproduce online content, posting an illegal or harmful material can cause butterfly effect. Once it is on the Internet, it is there almost forever. Impossibility to remove it from cyber space completely is another issue. People can download, edit and re-upload the edited versions to many different platforms in a very short time. To make things worse, due to the availability of wide range of anonymizers, it is not easy to find out the responsible individuals. This situation is less complicated with other media. Therefore restrictions on the right to free speech on the Internet should be considered more carefully.

This argument does not suggest either blocking the entire blog website because of an objectionable content in a single page or holding service providers liable for the user content, because, as in the China and Iran cases, such attempts lead to self censorship which is a huge obstacle in front of the freedoms on the net. On the contrary, authorities should consider the diverse and complicated nature of cyber space, observe the proportionality principle and ensure the basic legal provision to prosecute acts of defamation or involvement in execution videos are in place.

To conclude, as it was argued above, applying existing regulations to the Internet can be misleading. Internet is not less invasive compared to the other electronic media. However it does not have regional borders and it is not very easy to track down the owners of objectionable contents because of anonymity. Given that it is possible to post something offensive using someone else's name, accountability of actors is more delicate issue than it is on other media.

3.2 Infringement of Intellectual Property Rights

In this chapter, firstly how the Internet contributed to the online piracy will be investigated. Those contributions will be supported with the findings of several reports of different organizations. After that with the attempts of several countries to fight against this online tort, government's and industry's efforts in Turkey will be studied in order to compare with other developed countries. Before all of that it might be a good start to mention what Internet did for copying and distributing the copyrighted materials.

'Internet is the most effective copying machine ever invented.' (Steinmueller, 05/05/2012) Every bit of data including copyrighted works can be copied relatively easily at a few keystrokes via numerous tools. Unlike the old technologies, copying something over Internet is cheap and without a considerable effort. Just like electricity, copies of files flow through the communication paths very fast and reach a huge number of individuals at once immediately.

Therefore the Internet can also be characterized as the largest threat to copyright holders, because free flow of copies prevents creators from making money and discourages them from producing more. Software, novels, graphics, photos, movies, songs and other forms of digitized creative works are all copied and distributed by many people without authorization of the right holders every second. This threat has accelerated since the inception of the peer to peer applications, which enable individuals to locate a shared content file on another networked device and copy the material to its own hard drive. It is quick, effective and does not require the permission of the individual at the other end, assuming that necessary configurations are done in order to allow networked people to connect and download. Besides alternative forms of illegal distribution such as cyber lockers, illegal streaming services and forums in which links to copyrighted content are shared illegally by individuals are also serious and growing problems. Some figures might be useful to underline the severity of the issue. Findings of the International Federation of the Phonographic Industry (IFPI) and BSA about internet piracy represent the concerns of the industry.

According the 2011 Report of IFPI on Digital Music Sales:

> *Despite the surge by more than 1000 per cent in the digital music market from 2004 to 2010 to an estimated value of US$4.6 billion, global recorded music revenues declined by 31 per cent over the same period. The two figures powerfully illustrate how, in the face of piracy, even the most progressive strategy of licensing hundreds of digital music services has been unable to prevent the steady decline in the overall legitimate music market and that decline will continue unless action is taken.*

BSA illustrates a similar picture in 2010 Software Piracy Study:

> *The commercial value of software piracy grew 14 percent globally last year to a record total of $58.8 billion. While the number of PCs shipped to emerging economies accounted for 50 percent of the world total in 2010, the value of paid software licenses in emerging economies accounted for less than 20 percent of the world total.*

For the movie industry, 'a study found that in 2005 major studios in the United States lost $1.3 billion due to piracy. Of this, $447 million was attributed to Internet piracy with the remaining amounts coming from physical copies of movies sold by professional bootleggers.' (Smith and Telang, 2010:290)

Both of the reports conclude that media intermediaries and governments should take action against piracy. Website blocking at ISP level under the control of governments, search engine filtering, monitoring the p2p channels to tackle unauthorized downloads and redirecting users to warning pages are recommended as effective solutions. The attempts of French Government against digital piracy, HADOPI, are praised and some numbers are given to illustrate that governmental actions make significant differences. IFPI's latest report claims that:

> *official digital music sales saw a significant uplift at exactly the period when awareness of Hadopi was at its highest, in Spring 2009, when the law was being debated in the National Assembly. Music sales were 22,5% higher for singles and 25% higher for digital albums than they would have been, on average, in the absence of HADOPI.*

Also it is mentioned that usage of peer to peer applications decreased by 26% since October 2010.

However some argue that blocking websites or taking more strict precautions such as disconnecting individuals from Internet because of piracy concerns undermines consumers' ability to discover and evaluate media products. Media companies have disproportionately focused on the negative effects of the broadband Internet penetration and file sharing platforms. (Smith and Telang, 2010:296)

> *Pirated content available online can make users aware of the availability of certain movies and artists and eventually lead to purchases by users. Also file sharing networks can actually reduce search costs for users and can make them aware of more obscure and less advertised movies, leading to an increase in DVD purchase. (Smith and Telang, 2010:292)*

Furthermore it is argued that P2P networks can help sales of less popular digital products by reducing the search costs and providing samples. There is some literature studying the effects of search costs on the sales of digital products. (Brynjolfsson et al., 2007:26, Smith and Telang, 2010:292) However there is not enough literature and evidence on the magnitude of file sharing's contribution, in other words *sampling and advertising via piracy*, on media sales. In other words, it is not clear how many people decide to pay for the copyrighted content right after they view the pirated version.

Therefore, comparing the potential positive impact of advertising via piracy on the industry with the evident decreases in digital product sales because of unauthorized downloads does not seem a fruitful approach. However suggesting that peer to peer channels should be monitored to tackle the copyright breaches or that cyber lockers such as Rapidshare or Hotfile should be blocked to support the industry is not a fruitful perspective, either. Such decisions are fundamental right issues. Moreover, limiting or blocking the Internet traffic of P2P users, or, as an interesting suggestion, establishing general tax on veteran internet users that wish to pursue downloading and redistributing the revenues of the tax among copyright owners (Wong et al.,2011, 470) might cause network neutrality problems.

Besides facilitating online piracy, the services mentioned above also provide legitimate communication channels to countless individuals. In order to support the industry, there might be lessons to learn from the French case. Establishing an authority which is formed of representatives of all related actors in the industry can be a part of the solution. It can collect the reports, evaluate the situations and run the notice take down procedures. One of the most important things while forming such institutions is making them accountable for their actions.

There is another aspect of the French case which should be avoided. As it was argued before, disconnecting people from the Internet because of several copyright infringements is the violation of basic human rights. Even if one person repeats the offense despite the official notifications, assuming that other people might be sharing the same connection, disconnecting the line after two notifications discriminates all of them from the digital world. This argument does not support such sanctions in absence of sharing, either.

In Turkey, infringement of intellectual property rights did not take place in the Law No. 5651 which regulates the crimes committed via the Internet. Therefore, copyright holders, companies or organizations such as Turkish Phonographic Industry Society (MÜYAP) apply for court orders to block the websites which host objectionable content or to be able to remove such materials. Here are some examples of such attempts:

- On 19 September 2009, Beyoğlu Public Prosecutor's Office issued court orders to block LastFM and MySpace due to online copyright infringement claims upon the application of MÜYAP.
- On 29 December 2010, another court order was issued by Beyoğlu Public Prosecutor's Office to block one of the biggest music search engines Fizy.com upon the application of MÜYAP.

There is no safe harbour for such service providers in Turkey. Considering that those websites rank in the top visited websites in many countries, such decisions do not follow the principle of proportionality. Since the rise of Web 2.0 technologies which allow Internet users to create and share any content with each other in a social media dialogue, this issue has been more complicated. Given that service providers cannot monitor all of the activities of their users, blocking the entire website due to existence of an infringing material posted by a user negatively influences not only the provider but also other users. Therefore regulations are necessary to protect major service providers on the Internet from the liability for the activities of their users.

For example, United States' Digital Millennium Copyright Act of 1998 offers a *conditional safe harbour* to service providers under certain circumstances. According to the Online Copyright Infringement Liability Limitation section, if service providers meet the following criteria, they are exempt from claims of copyright infringement made against them.

1. The transmission must be initiated by a person other than the provider.

2. The transmission, routing, provision of connections, or copying must be carried out by an automatic technical process without selection of material by the service provider.

3. The service provider must not determine the recipients of the material.

4. Any intermediate copies must not ordinarily be accessible to anyone other than anticipated recipients, and must not be retained for longer than reasonably necessary.

5. The material must be transmitted with no modification to its content.

In order to qualify for the safe harbour provisions, service providers' activities must also meet two additional conditions. First condition is that 'service provider must adopt and reasonably implement a policy of terminating in appropriate circumstances the accounts of subscribers who are repeat infringers.' This condition is like the third step of HADOPI law. Secondly:

> *service providers must accommodate and not interfere with standard technical measures which are defined as measures that copyright owners use to identify or protect copyrighted works, that have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair and voluntary multi-industry process, are available to anyone on reasonable non-discriminatory terms, and do not impose substantial costs or burdens on service providers.*

This law also requires service providers to designate an agent to whom notices of copyright infringement can be sent. In this regard this law can be considered useful, because procedures can be executed more quickly. However one might think that this places a lot of power in the hands of regulatory agents.

In Turkey the agents of service providers are only responsible to courts and Telecommunications Presidency (TİB) under the Information and Communication Technologies Authority (ICTA). The Telecommunications Presidency coordinates notice-take down procedures from one centre. Given that the infringement of IPR is not listed as a crime in Law. 5651, it is considered to be a secondary issue in terms of administrative blocking orders, unless there is a court order sent to the TİB. Courts can send orders either to TİB or directly to ISPs. Assuming that running the notice and take down procedures through court orders takes long time; this mechanism needs to be developed in order to respond to the needs of the industry better.

3.3 Pornography, Child Abuse and Parental Control

The word pornography comes from the ancient Greek porné and graphos, which literally translates as writing about prostitutes. However, in the modern context the term has taken on a new meaning and materials considered as pornographic do not necessarily have to be neither written, nor about prostitutes. Nowadays it is generally used to describe sexually explicit, written or visual material including books, photographs, magazines, films and any online material which is primarily designed to produce sexual arousal in viewers. (Caroline, 2008:4) It is a very controversial issue in almost every country. 'Some lawyers and political philosophers consider the problem of pornography to be the problem of freedom to speak unpopular or wicked thoughts.' (Dworkin, 1981:177) Some approach to the issue from a feminist point of view and claim that women are subordinated and harmed via pornography, therefore such materials violate women's fundamental human rights. In her famous book called Sex Equality, Catharine A. MacKinnon states that:

> *Pornography is a discriminatory practice based on sex which denies women equal opportunities in society. Pornography is central in creating and maintaining sex as a basis for discrimination. Pornography is a systematic practice of exploitation and subordination based on sex which differentially harms women. The bigotry and contempt it promotes, with the acts of aggression it fosters, harm women's opportunities for equality of rights in employment, education, access to and use of public accommodations, and acquisition of real property, promote rape, battery, child abuse, kidnapping and prostitution and inhibit just enforcement of laws against such acts, and contribute significantly to restricting women in particular from full exercise of citizenship and participation in public life. (MacKinnon, 2001:1562)*

On the other hand, although they do not approve pornography personally and find it low value speech which contributes little, if anything, of intellectual, artistic, literary or political merit to the moral and social environment, there are liberal defenders of pornography, too. Those also find especially violent and degrading forms of sexually explicit materials mindless and offensive. However, they strongly oppose to the restrictions of such content stating that:

> *mentally competent adults must not be prevented from expressing their own convictions, or from indulging their own private tastes, simply on the grounds that, in the opinion of others, those convictions or tastes are mistaken, offensive or unworthy. Moral majorities must not be allowed to use the law to suppress dissenting minority opinions or to force their own moral convictions on others. (Caroline, 2008:28)*

Actually it is a dangerous oversimplification to claim that those who argue in favour of censorship of pornography ground their arguments on their personal opinions that such actions are mistaken or offensive. There are many cases which prove pornography causes serious harms to people. Here is an example:

Pornography not only has a role in sexual assaults by strangers. It also causes sexual abuse and violence at home. Pornography is often used against women by boyfriends and family members as a manual for their abuse. (Evans, 2005:46) A victim of such case testified as follows:

> *My father incestuously abused me for a period of 10 years, from the time I was 8 years old until I was 18. During the early ages of the molestation, my father used pornographic materials as a way of coercing me into having sex with him. He used pornography for several purposes. First of all, he used it as a teaching tool – as a way of instructing me about sex and about what he wanted me to do with him. When he showed me the pictures, he would describe the acts in details. Second, my father used the pictures to justify his abuse and to convince me that what we were doing was normal. The idea was that if men were doing it to women in the pictures, then it was OK for him to do it to me. Finally, he used the pornography to break down my resistance. The pornography made the statement that females are nothing more than objects for men's sexual gratification. How could I refuse my father when the pornography showed me that sex is what women and girls are for? (Brady, 1993:43)*

In this case victim claims that pornography was the catalyst of sexual violence. Moreover, pornography can have negative consequences for both the user and his or her intimate partner. Some of the common damaging effects of pornography for users can include addiction, isolation, increased aggression, distorted beliefs and perceptions about relationships and sexuality, negative feelings about themselves, and neglecting other areas of their lives. (Maltz & Maltz, 2006:72) Therefore the negative effects of pornography are not just personal opinions, as the liberal defenders of pornography claim. Consequences of exposure to pornography on adults are not the focal point of this chapter. The damaging effects mentioned above were given to illustrate that considering that even adults are vulnerable to such content, the effects of pornography on children can be much more catastrophic. Research suggests that 'when one thought is activated, other thoughts strongly connected to that thought are also activated. Aggressive ideas in violent programs are believed to activate other aggressive thoughts in viewers through their association in memory pathways.' (Benedek & Brown, 1999:238) The authors of the same article also state that 'by interference, sexual activity heard or seen on television' or Internet as more likely example nowadays 'may stimulate other sexual ideation in young children.' Also it is highlighted that 'the potential harm may include changes in other domains, such as attitudes, morals, values, family or community relationships, and psychological and emotional wellbeing.' (Benedek & Brown, 1999:238)

Findings of a research conducted in USA among 1,501 children aged between 10 and 17 years old, indicate that '25% of the children regularly using the lnternet had one or more unwanted exposures to sexual images. Most of the exposures occurred during Internet searches at home, *the majority being non-voluntary*.' (Flander et al., 2009:849) 'Responses relating to emotional reactions state that in 24% of cases children reported being upset or exceedingly distressed by the exposure, and 19% of children had at least one symptom of stress.' (Flander et al., 2009:850)

In many countries including Turkey, pornographic materials such as magazines and films are exhibited in opaque plastic bags in private areas so that they are not advertised to children. Turkish Criminal Code Article 226 clearly states that those who display, advertise or sell pornographic materials to minors are sentenced to jail terms from six months to two years. The law does not mention the Internet specifically but clearly states that all kinds of media are subject to Article 226. Considering that Internet offers more risks to children and youth than any other media, developing measures to diminish exposure to pornography in cyberspace is vital. Unfortunately installing filtering software on personal computers by parents is not enough. Because 'a generation gap exists between parents and children in terms of knowledge about computers and the Internet in particular, with children being more computer savvy.' (Odabaşı and Çankaya, 2009:1108) When it is about protecting children, pomography is not the whole story.

Findings of a research conducted in New Zealand about unsafe Internet usage among children points to the necessity of action plans. (Valcke et al., 2007:2840) The research involved 347 girls between 11 and 19 years old. According to the results,

- 29% sent mail and 26% got in touch via phone calls with people they met via the lnternet.

- 33.5% did personally get in touch with strangers they met via the Internet.

- 34.5% did not tell their parents about getting in touch with strangers via the Internet.

- 60% had used at least once the Internet in an unsafe way; i.e. passing on their name, address, phone number, or pictures.

- 75% of the girls indicate they are being controlled only occasionally by their parents as to their Internet usage and 37.5% reports never being controlled.

- 22.5% reports that they have felt threatened while using the Internet.

Therefore Internet provides child abusers with abundance of new possibilities. 'Similar findings of another study, indicate that 31% of children and youth aged 10–17 reported viewing web pages with pornographic material, even if accidentally. One out of every five children reports having experience that someone wanted to get close to them sexually, and one out of 30 reports that this provocation was aggressive.' (Flander et al., 2009:850)

Parents take different precautions to protect their children from online dangers. Some do it by limiting online hours (62%), whereas others use software to filter or block questionable websites (32%). Almost every parent states that they keep an eye on children's Internet use (91%). However the same research found that 55% of children aged between 12 and 15 years old stated that they did not tell their parents everything they did on the Internet. (Çankaya and Odabaşı, 2009:1108)

As a result, it is obvious from the data that parental control needs to be supported by more comprehensive solutions which involve ISPs, institutions and governments. Therefore this is an open ended issue which seems to attract more attention of rivals as governments develop more regulations.

4. ANALYSIS OF ONLINE CONTENT REGULATIONS IN TURKEY

In this chapter two important pillars of Turkish online regulations trajectory will be investigated. The first one is the Law 5651 which criminalizes some of the online actions, whereas the second regulation provides families an optional and customizable filtering service called Safer Internet Service. In each regulation liabilities of actors, major cases and public response will be studied and compared to the previously studied countries.

Turkey's Internet regulations started in 2007, when the government enacted Law No. 5651, entitled 'Regulating Broadcasting on the Internet and Fighting Crimes Committed through Internet Broadcasting'. The law aims to combat certain online crimes such as promoting prostitution, encouragement and incitement of suicide, facilitation of the use of drugs, obscenity, and regulates procedures regarding such crimes committed on the Internet through content, hosting, and access providers.

The second major regulation was the Safer Internet Service which was launched in November 2011 to protect children and youth from harmful content on the Internet. This optional service is provided by ISPs free of charge upon the request of subscribers. Consisting of two profiles named Family and Child, Safer Internet Service aims to help families control their Internet usage within the house.

Details of both legislations are given below.

4.1 Law No. 5651: Regulating Broadcasting on the Internet and Fighting Crimes Committed Through Internet Broadcasting

The Turkish Government enacted the Law on 4 May, 2007. Until then the Internet was considered the same as other media and regulated under the same terms, but this law provided further specifications as to what was not allowed online. The explanatory note of the Law referred to article 41 of the Turkish Constitution states that, 'the state shall take the necessary measures and establish the necessary organisation to ensure the peace and welfare of the family, especially where the protection of the mother and children is involved.' (Akdeniz, 2009:7)

According to the Article 8 also known as the categorization of online crimes, websites which host particular contents can be blocked and those who publish such content are subject to certain penalties. Every item under Article 8 refers to particular article of Turkish Penal Code (TPC). The eight categories of crimes under the Article 8 are:

1. Encouragement and incitement of suicide (Article 84 of the TPC)
2. Sexual exploitation and abuse of children (Article 103 of the TPC)
3. Facilitation of the use of drugs (Article 190 of the TPC)
4. Provision of dangerous substances for health (Article 194 of the TPC)
5. Obscenity (Article 226 of the TPC)
6. Promoting prostitution (Article 227 of the TPC)
7. Providing Opportunities and Places for Gambling (Article 228 of the TPC)
8. Crimes committed against Atatürk the founder of the Turkish Republic.

Telecommunications Presidency (TIB) within the Information and Communication Technologies Authority of Turkey is responsible for executing blocking orders issued by judges, courts and public prosecutors. Under the same law, the Presidency was also given the authority to issue administrative blocking orders. If a website whose content falls into the scope of Article 8 is hosted within Turkey, notice and take down procedures are followed. Otherwise such websites are blocked through national DNS servers or routers. All decisions of the Presidency and other authorities can be challenged at administrative courts.

4.1.2 Liabilities of Actors

All ISPs have to execute the blocking orders sent by TIB or a court no later than twenty four hours. Here it is worth noting that blocking orders can be sent by TIB or a public prosecutor, judge or a court directly.

> *The directors of hosting and access providers who do not comply with the blocking orders issued through a precautionary injunction by a Public Prosecutor, judge, or a court, could face criminal prosecution and could be imprisoned between 6 months to 2 years under Article 8(10). (Akdeniz, 2009:8)*

Moreover under the Article 8(11) it is stated that:

> *access providers who do not comply with the administrative blocking orders issued by TIB could face fines from EUR 4600 to EUR 46000. Also if an access provider fails to execute the administrative blocking order within twenty-four hours of being issued an administrative fine, the Telecommunications Authority can revoke the access provider's official activity certificate. (Akdeniz, 2009:8)*

4.1.3 Major Cases

The most famous example of website blocking under the Law 5651 is the Youtube case. On 5 May, 2008, Ankara 1st Criminal Court of Peace issued a court order to block the famous video sharing platform regarding to the defamatory videos of Atatürk and the Turkish flag. The website remained blocked within the country for two and a half years, because the company refused to remove those videos from its website within this period. In October 2010, the same court issued an order for the removal of the ban, because Youtube removed the related videos from its website. Youtube case was criticised as the court order was deemed to be disproportionate and it was an example of content blocking based on political reasons.

Another example is the administrative blocking order of TIB dated 2 November 2009, with regards to Gabile.com and Hadigayri.com, 'which combine to form the largest online gay community in Turkey, at approximately 225.000 users.' (Akdeniz, 2009:16) TIB stated that those websites were blocked because of 'the suspicion of promoting prostitution' based on Article 8(6). After the websites had made the necessary technical changes as TIB requested, they were made accessible to Internet users again. Many academics object to the administrative blocking orders issued by TIB stating that those orders lack from transparency as TIB does not publish the list and underlying reasons of such orders. (Memiş, 2009:175, Akdeniz, 2009:20)

4.2 Safer Internet Service

On 22 November 2011, ICTA launched another important pillar of Turkish Online Regulations, named Safer Internet Service. Subscribers who want filter their Internet traffic according to the predefined profiles can benefit it free of charge. If subscribers do not want to use this service, their traffic will not be filtered. Also if a subscriber who benefit from the service is not satisfied with it or does not want to use it anymore for any reason whatsoever, he can abandon the service anytime he wants.

There are two profiles under the Safer Internet Service called Family and Child, under which certain types of websites are filtered. If a subscriber chooses Family profile, websites which host objectionable content become inaccessible to the user. Those objectionable contents are obscenity, gambling, prostitution, racism, violence, terrorism, malicious software and all crimes under the Article 8 of the Law 5651. The database of objectionable websites is maintained and updated by TIB and sent to the ISPs regularly. Also Family profile provides three more options to subscribers. Websites which offer online gaming, social networking and instant messaging services can be filtered upon the preference of the subscriber. The service is criticised by media, because the filtering criteria of objectionable websites such as violence is claimed to be ambiguous. On the same day of service launch, one of the major national newspapers called Milliyet published a report in which critics of several actors in the online industry are presented. (Milliyet, 22/11/2011) The common point on which those actors agree on is that filtering criteria is not defined publicly and TIB does not incorporate all related actors into the decision making processes. TIB responded to such critics on the official website of Safer Internet Service, stating that filtering criteria is defined by a committee consisting of psychologists, pedagogues, sociologists and legal advisers.

The second profile is called Child which offers a narrower list of accessible websites compared to the Family profile. Again, the criteria of accessible websites are defined by the committee and the database is maintained by TIB and sent to ISPs and mobile operators regularly.

Lastly subscribers who benefit from the service can switch between the profiles or abandon the service through a website anytime they want by using the credentials provided by their ISPs or they can do it by calling the customer services. Mobile operators also supported the switching operations with SMS.

4.2.1 Liabilities of Actors

The Internet Department of Communications Presidency is responsible for maintaining and updating the black and white lists of websites according to the predefined criteria of the committee. Also the authority is responsible for monitoring whether the ISPs and mobile operators apply the updates to their filtering systems regularly.

On the other hand, all ISPs and mobile operators have to install a filtering system, so that they can offer the Safer Internet Service to their operators. Costs of installation, maintenance and operation of those systems belong to the service providers. Once the systems are up and running, they must receive the updates from TIB servers and apply them to their own servers. On the customer side, ISPs have to create a website in which internet users can switch between profiles and abandon the service if they want to. Moreover through those websites, ISPs must provide users with brief information of the profile switching history, so that users can monitor whether their credentials are being used by another member of the family beyond the subscribers' control.

Customers, on the other hand, are responsible for keeping their credentials safe and secure. When they encounter a website which is not accessible under the their profile and think that that website should not be prohibited, they can report it to the authority in order to remove it from the black list by filling a simple form at the end of the warning page. Other than that, they can report harmful websites to the authority as well.

4.2.2 Feasibility

Maintaining and updating the black and white lists (accessible websites of the Child profile) is the main challenge of this service. Given that every second thousands of websites are born and die, even if the authority can categorize the database of all domain names obtained from a registrar, updating it is another story. Therefore it is not realistic to claim that profiles work 100% efficient. However, categorising the prominent websites such as the most visited one hundred thousand websites by Turkish people might serve, as most of the Internet users are using them. Also considering that databases are supported by the reports of Internet users, the situation seems to be less problematic, but this circle is a serious resource consuming process which never ends.

4.2.3 Social Challenges and Puhlic Response

When the President of ICTA, Tayfun Acarer, announced that Safer Internet Service will be launched by the end of the year at a press conference on 5 May 2011, it sparked one of the hottest debates of the year. It is difficult to find comprehensive academic papers which discuss the pros and cons of the service so far. However an NGO called Alternative Informatics Organization (AIO) published a report which was signed by 175 academics stating that such a filtering mechanism leads to censorship as it is designed to be *central, arbitrary and non-transparent*. The report addresses to the computer literacy as a solution to the Internet torts. Also, there was a considerable amount of interest about the concerns of different parties in domestic and foreign media. According to a CNN World report, 'critics argue that it is not clear how the filtering system will work.' (CNN World, 15 May 2011)

On the other hand, another report published in one the major national newspapers questioned the political tension between online safety and fundamental rights. The report concluded the service to be a positive attempt to protect children as long as it is optional and the filtering criteria is transparent. (Çopur, 21 May 2011)

The most noteworthy protest happened on 15 May 2011, a week after the announcement of the service. Several thousands of protestors, who argue that that service is a kind of discrimination that the government wants to monitor online behaviours, occupied the Taksim Square in Istanbul carrying signs reading 'Don't Touch my Internet'. Also, the cyber-activist group called Anonymous attacked to the servers of the Communications Presidency on 9 June 2011 to protest the service arguing that the new filtering service is the violation of one of the most fundamental rights, freedom of communication. As the servers were reported to be not affected because of the attack, the Presidency did not start take action in response to this. Since then, no such protest happened against the service.

Meanwhile, according to the statements of the President of ICTA posted on the website of TIB, 5 millions of Internet users have been using the Safer Internet service since 22 November 2011, the date of service launch. That number suggests that the service is appreciated among home users, considering that there are approximately 35 millions of Internet users in Turkey according to the ITU report, entitled 'Individuals Using the Internet 2000-2011.'

5. POLICY SUGGESTIONS

The research question of this study is how Turkey should proceed with online regulations. Below, some policy suggestions are introduced to answer this question.

The social response and academic opinions numerously state that Turkey's online regulations must be saved from certain ambiguities. Article 8 of the Law 5651 mentions 'sufficient suspicion' is required to maintain a legal base for website blockings. The boundaries this term must be drawn clearly in order to prevent censorship. Otherwise this situation might lead to self regulation policies. Countries such as China and Iran which employ extreme censorship policies can be good examples of this argument. Moreover the scope of administrative blocking orders issued by TIB should be clarified. The more questions about the reasons of administrative blockings are left unanswered, the less the regulations are supported by the public.

Another point which requires clarification is the filtering criterion of the Family and Child profiles of the Safer Internet Service. On its website, TIB offers a service through which people can query which website belongs to which profile. Also, as mentioned before, the Presidency states that the filtering criterion have been developed by a committee consisting of experts of their respected fields. Those are affirmative steps for transparency. However including NGOs to such decision making processes can increase the reputation and the quality of the services.

Turkish authorities should consider age verification systems more rather than blocking objectionable websites such as those publishing violent materials. As in the Australian regulations, allowing websites which use authorized age verification systems might help parents protect their children better. However, since the level of computer literacy increases among minors, they can always find ways to circumvent filtering. Therefore website owners must be included in the development of the regulatory framework, too.

6. CONCLUSION

Dialogs on Turkish online content regulations are still going on. As in most of the developed world, there is not a perfect consensus on cyber matters. The Law 5651 attempts to fill the legal gap on Internet during the fight against cyber torts, while Safer Internet Service is intended to improve the protection of children. As in the cases of many developed countries discussed before, Turkish authorities embrace a modular approach for online regulations. Instead of broadening the scope of Article 8 of Law 5651, demands of families who seeking a *cleaner* Internet usage are satisfied by another optional, free service called Safer Internet Service. The motto ‘choosing is freedom’ of this service is put in front of the opponents of online filtering. People who do not want to use the service are only restricted to the applications of Article 8, whereas families who do not want to encounter any kinds of obscenity or other online dangers can limit their Internet to a safer zone by using Safer Internet Service. This approach is plausible, since the choice of some people do not affect others’ freedoms.

Moreover Turkish authorities obviously embrace the Internet in which penal code applies. Therefore the argument, ‘none of the filtering attempts, website blockings and whatsoever are acceptable in terms of fundamental rights’ is not respected. Actually such claims are not supported in any of the developed countries, either. The chapter of this study, in which online regulations of several countries are evaluated, clearly states that fundamental rights also have limits and this applies to the Internet as well.

However different actors complain about being not included to decision making processes in Turkey. If authorities neglect such claims and develop online regulations in a sealed box, the situation might lead to catastrophic consequences, like Iran and People’s Republic of China. Therefore, along with including key actors, authorities should focus on the points such as clarifying the details of the filtering criterion of the Safer Internet Service, defining the boundaries of administrative blocking orders etc. which can help develop more transparent regulations.

In conclusion, considering the characteristics of the country’s online regulations, Turkey can be classified as a moderate censor.

BIBLIOGRAPHY

1. Marx, G. T., "Censorship and Secrecy: Legal Perspectives", International Encyclopedia of the Social & Behavioral Sciences, 2001, pp. 1581-1588.
2. Reinhard, C., "At the Edge of Information: Changing Ethical Dilemmas - The Ethics of Censorship: Should Governments Cover Our Children's Eyes", Ethica Publishing, Colorado, 2007, pp. 164-172.
3. Dutton, H. W., Dopatka, A., Hills, M., Law, G., Nash, V., "Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet", UNESCO Publishing, Paris, 2011. (Available at: http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/freedom-of-connection-freedom-of-expression-the-changing-legal-and-regulatory-ecology-shaping-the-internet/. Date of Access: 20/06/2012)
4. Almagor-Cohen, R., "The Scope of Tolerance: Studies on the Costs of Free Expression and Freedom of the Press", Ethical Space: The International Journal of Communication Ethics, Vol:3, No:1, pp. 12-14, London, 2006.
5. Sussman, L. R., "Censor dot gov: the Internet and Press Freedom", Journalof Govemment Information, No. 27, pp. 537-545, Newyork, 2000.
6. Bittlingmayer, G., Hazlett, T., "Open access: The Ideal and The Real", Telecommunications Policy, No: 26, pp. 295-310, USA, 2002
7. Wong, S., Altman, E., Mora, J. R., "Internet Access: Where Law, Economy, Culture and Technology Meet", Computer Networks, No: 55, pp.470-479, 2011.
8. Lievens, E., "Protecting Children in the New Media Environment: Rising to the Regulatory Challenge?", Telematics and Informatics, No: 24, pp.315-330, 2007
9. Gevers, M. d'U., Poullet, Y., "Concerns from a European User Empowerment Perspective About Internet Content Regulation: An Analysis of Some Recent Statements-Part I", Computer Law & Security Report, Vol: 17, No:6, pp. 371-378, 2001.
10. Akdeniz, Y., "To Block or not to Block: European Approaches to Content Regulation and Implications for Freedom of Expression", Computer Law & Security Review, No: 26, pp. 260-272, 2010.

11. Cheung, A. S. Y. "The Business of Governance: China's Legislation on Content Regulation in Cyberspace", China and The Internet Conference in Los Angeles, 2006 (Available at: https://docs.google.com/viewer?a=v&q=cache:JTe_8J1WECEJ:www.law.nyu.edu/idcplg?IdcService%3DGET_FILE%26dDocName%3DECM_DLV_015050%26RevisionSelectionMethod%3DLatestReleased+china+internet+content+regulation&hl=tr&gl=tr&pid=bl&srcid=ADGEESgUxOdm4T9B27vEluxdeZ6GfnfHlt8qwNW6Zloh47sDFZcgM_UyNIY-jxuwzRr0yDJBafF_ebpaOFLKY2ci8DUk2whlzQ8lVvWRyJq1CgNuNbFtw2hXyVHD9jzjiRbseaMgVFSk&sig=AHIEtbSOMAtD-u2K-DiTs37DIGK1vmgzAw. Date of Access: 23/06/2012)
12. Tan, Z., Mueller, M., Foster, W., "China's New Internet Regulations: Two Steps Forward, One Step Back", Communications of the ACM, Vol:40, No:12, pp.11-16, 1997.
13. Surborg, B., "Online with the people in line: Internet development and flexible controlof the net in Vietnam", Geoforum, No:39, pp. 344-357, 2008
14. Shirazi, F., "Free and Open Source Software versus Internet Content Filtering and Censorship: A Case Study", The Journal of Systems and Software, No:85, pp. 920-931, 2012.
15. Lievens, E., "Protecting Children in the New Media Environment: Rising to the Regulatory Challenge", Telematics and Informatics, No:24, pp.315-330, 2007.
16. Diebert, R., Palfrey, J., Rohozinski, R., Zittrain, J., (Ed.), "Access Denied: The Practice and Policy of Global Internet Filtering", The MIT Press, USA, 2008
17. Akdeniz, Y., "Internet Content Regulation: UK Government and The Control of Internet Content", Computer Law & Security Report, Vol: 17, No:5, pp. 303-317, 2001.
18. Clayton, R., "Anonymity and Traceability in Cyberspace", Technical Report, No: 653, University of Cambridge Press, 2005.
19. La Rue, F., "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", UN Human Rights Council, 2009. (Available at: http://www.unhcr.org/refworld/docid/49f8416d2.html, Date of Access: 26/06/2012)
20. Diebert, R., Palfrey, J., Rohozinski, R., Zittrain, J., (Ed.), "Access Controlled", The MIT Press, USA, 2010.

21. Armstrong, W., S., "Legal Interpretation in Democratic States: Two Ways to Derive Constitutional Rights", pp. 231-244, Australia, 2002.

22. Naisbitt, J., "*Megatrends: ten new directions transforming our lives*" New York: Warner Books, New york, 1982.

23. ICTRC (Iran's Civil Society Organizations Training and Research Centre), Report on the Status of Internet in Iran, (Available at: http://www.genderit.org/sites/default/upload/A_Report_on_Internet_Access_in_Iran_2_.pdf, Date of Access:03.07.2012)

24. Human Rights Watch, "Human Rights Issues Regarding the Islamic Republic of Iran", 2011. (Available at: http://www2.ohchr.org/english/bodies/hrc/docs/ngos/HRW_Iran_HRC103.pdf, Date of Access: 03.07.2012)

25. Jacobs, F.G., White, R.C.A., "The European Convention on Human Rights", Clarendon Press, Oxford, 1996.

26. Jorgensen, R. F., "Internet and Freedom of expression", Raoul Wallenberg Institute: European Master Degree In Human Rights And Democratisation, Sweden, 2001. (Available at: www.ifla.org/files/faife/publications/ife03.pdf, Date of Access: 06/07/2012)

27. The Committee of Ministers, "Declaration on Human Rights and The Rule of Law in the Information Society, The 926th meeting of the Ministers' Deputies, 13 May 2005. (Available at: https://wcd.coe.int/ViewDoc.jsp?id=849061, Date of Access: 06/07/2010)

28. Montero, E., Enis, Q., "Enabling Freedom Of Expression In Light Of Filtering Measures Imposed On Internet Intermediaries: Squaring The Circle?", Computer Law & Security Review, No:27, pp. 21-35, 2011.

29. Rowland, D., Macdonald, E., "Information Technology Law", Cavendish Publishing, London, 2005.

30. Paul, E. F., Miller, F. D., Paul, J., "Freedom of Speech", Cambridge University Press, Cambridge, 2004.

31. Price, M. E., "Media and Sovereignty: The Global Information Revolution and Its Challenge to State Power", The MIT Press, USA, 2002.

32. Livingstone, S., Magdalena, B., Helsper, E., "Internet Literacy Among Children And Young People: Findings From The UK Children Go Online Project", LSE Research

Online Report, (Available at: http://eprints.lse.ac.uk/archive/00000397, Date of Access: 07/07/2012)

33. Steinmueller, E., "Governing the Internet", Information and Communication Technology Policy and Strategy Lecture Week 9, University of Sussex, UK, 2012.
34. IFPI, "Digital Piracy: Facts and Trends", Digital Music Report 2011, (Available at: http://www.ifpi.org/content/library/DMR2011.pdf, Date of Access: 09/07/2012)
35. IFPI, "Digital Piracy: Facts and Trends", Digital Music Report 2012, (Available at: www.ifpi.org/content/library/DMR2012.pdf , Date of Access: 09/07/2012)
36. BSA, "Piracy Study", 2011,
(Available at:
http://portal.bsa.org/globalpiracy2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf, Date of Access: 09/07/2012)
37. Smith, M. D., Telang, R., "Piracy or promotion? The impact of Broadband Internet Penetration on DVD Sales", Information Economics and Policy, No:22, pp. 289-298, 2010
38. Brynjolfsson, E., Hu, Y., Simester, D., "Goodbye Pareto Principle, Hello Long Tail: The Effect of Search Costs on the COncentration of Product Sales", 2007. (Available at: http://faculty.washington.edu/mfan/is582/articles/Hu2007.pdf, Date of Access: 09/07/2012)
39. West, C., Zalta, E. N. (ed.), "Pornography and Censorship", *The Stanford Encyclopedia of Philosophy, 2008,* (Available at: http://plato.stanford.edu/archives/fall2008/entrics/pornography-censorship, Date of Access: 11/07/2012)
40. MacKinnon, C. A., "Sex Equality", Foundation Press, New York, 2001.
41. Pacillo, E. L., "Note: Getting a Feminist Foot in the Courtroom Door. Media Liability for Personal Injury Caused by Pornography", Suffolk University Law Review, No. 123, pp. 346-347, 1994.
42. Evans, M., "Regulating Internet Pornography As an Issue of Sex Discrimination", Murdoch University LLM Research, Australia, 2005.
43. Brady, K., Diana, E. H. (ed.), "Making Violence Sexy: Feminist Views on Pornography", Teachers College Press, pp. 43-44, Newyork, 1993.
44. Maltz, W., Maltz, L., "The Porn Trap: The Essential Guide to Overcoming Problems Caused by Pornography", Harper Collins Books, New York, 2006.

45. Çankaya, S., Odabaşı, H. F., "Parental controls on children's computer and Internet use", Procedia Social and Behavioral Sciences, No.1, pp. 1105-1109, 2009.

46. Valcke, M., Schellens, T., Keer, H. V., Gerarts, M., "Primary school children's safe and unsafe use of the Internet at home and at school: An exploratory study", Computers in Human Behaviour, No. 23, pp. 2838-2850, 2007.

47. Akdeniz, Y., "Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship", 2009.
(Available at: www.osce.org/fom/41091, *Date of Access: 20/07/2012*)

48. Memiş, T., "Erişimin Engellenmesi, Hukuki Sorunlar ve Çözüm Önerileri (Website Blocking, Legal Issues and Recommendations)", 2009.
(Available at: http:*//hukuk.erzincan.edu.tr/dergi/makale/2009%20XIII_2-9.pdf, Date of Access: 20/07/2012*)

49. Milliyet, "Safer Internet Service Launches Today", 22/11/2011. (Available at: http://teknoloji.milliyet.com.tr/guvenli-internet-donemi-basladi/internet/haberdetay/22.11.2011/1465897/default.htm
Date of Access: 21/07/2012)

50. The Official Website of Safer Internet Service, "What is in Safer Internet Service Profiles?", http://guvenlinet.org.tr/tr/menu/14-Profillerde_Neler_Var_.html, Date of Access: 21/07/2012.

51. Altemative Informatics Organization, "Academic Awareness Against the Filtering Service of ICTA and Call to University Rectors", 30/01/2012. (Available at: http://www.alternatifbilisim.org/wiki/BTK%27n%C4%B1n_Filtre_Uygulamas%C4%B1na_Kar%C5%9F%C4%B1_Akademik_Fark%C4%B1ndal%C4%B1k_ve_T%C3%BCm_%C3%9Cnv._Rekt%C3%B6rl%C3%BCklerine_%C3%87a%C4%9Fr%C4%B1, Date of Access: 23/07/2012)

52. Comert, Y., "CNN World Report: Marchers Protest new Turkish Web Filtering Rules", 15/05/2011,
(Available at: http://articles.cnn.com/2011-05-15/world/turkey.internet.protest_1_marchers-protest-internet-users-cnn-reporter?_s=PM:WORLD, Date of Access:23/07/2012).

53. Çopur, H., "22 Ağustos'da İnternet'e Sansür mü Geliyor?", 21/05/2011. (Available at: http://www.sabah.com.tr/Perspektif/2011/05/21/22-agustosta-internete-sansur-mu-geliyor, Date of Access: 23/07/2012)

54. Akdeniz, Y., "Governing Pornography & Child Pornography on the Internet: The UK Approach," in Cyber-Rights, Protection and Markets: A Symposium, University of West Los Angeles Law review, pp. 247-275, 2001.
55. United States International Trade Commission, "China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy", Investigation No. 332-519, 2011 (Online available at: http://www.usitc.gov/publications/332/pub4226.pdf, Date of Access: 17/07/2012)
56. Farivar, C., "The Internet of Elsewhere: The Emergent Effects of a Wired World", Ruthgers University Press, 2011.
57. Benedek, E., & Brown, C., "No excuses: Televised pornography harms children", *Harvard Review of Psychiatry,* 7(4), pp.236–240, 1999.
58. Haney, J. M., "Teenagers and Pornography Addiction: Treating the Silent Epidemic" VISTAS Online Articles, 2006. (Online Available at: http://counselingoutfitters.com/vistas/vistas_2006_Title.htm#TU, Date of Access: 10/08/2012)