UNIVERSITY OF ESSEX
SCHOOL OF LAW

LLM in Information Technology, Media and E – Commerce

2008 – 2009

Supervisor: Chris Marsden

DISSERTATION

INTERNET CONTENT REGULATION AND FREEDOM OF EXPRESSION: ASSESSMENT OF TURKISH CASE WITHIN THE FRAMEWORK OF THE ECHR

Name: YASİN BAKIRCI
Registration Number: 0808425
Number of Words: 19,965
Date Submitted: 11 SEPTEMBER 2009

CONTENTS

1. INTRODUCTION

The use of Internet services provides everyone with unmatched opportunities to express their opinions, and to distribute and access information freely. Values such as openness, transparency and efficiency, which are essential for a democratic society, can be realized by means of the Internet.[1] The Internet provides individuals with a novel instrument for imparting and searching for information.[2] Moreover, as a result of having a right to impart information, anyone can be a publisher on the Internet.[3]

However, opportunities stemming from using the Internet have been abused by malicious people, who use it as an instrument for illegal and harmful purposes. The Internet has become a safe-haven for activists who resort to unlawful means to attain their goals, because they see it as a lawless place. The Internet, emerging as a new environment for conventional crimes, has challenged certain democratic rights, such as privacy and freedom of expression.[4] It is believed that although respect for the right to freedom of expression is important, this right should not be seen as tolerating the promotion of 'sexual, racial or other forms of discrimination deemed contrary to the public good'.[5] Therefore, due to its negative effects on democratic rights, it has been considered vital to fight against illegal and harmful content on the Internet.[6]

---

[1] Bertelsmann Foundation, 'Self-regulation of Internet Content', Gütersloh, 1999, p.15, <http://www.cdt.org/speech/BertelsmannProposal.pdf>

[2] R. F. Jørgensen, 'Internet and Freedom of Expression', European Master Degree in Human Rights and Democratisation 2000-2001, Raoul Wallenberg Institute, 2001, p.5, <http://www.ifla.org/files/faife/publications/ife03.pdf>

[3] Global Internet Liberty Campaign, 'Regardless of Frontiers: Protecting the Human Right to Freedom of Expression on the Global Internet', <http://gilc.org/speech/report/>

[4] M. Kiškis, R. Petrauskas, 'Internet Content Regulation - Implications for E-Government', The Journal of Information, Law and Technology (JILT), 2005(2), <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2005_2-3/kiskis-petrauskas/>

[5] D. Capitanchik, M. Whine, 'The Governance of Cyberspace: Racism on the Internet', JPR/Policy Paper, No. 2, 1996, <http://www.jpr.org.uk/Reports/CS_Reports/PP_2_1996/index.htm>

[6] M. Marzouki, '10 Years of Internet Content Regulation in Europe: Empowering or Infantilizing Citizens?', 17th International Conference on Computers, Freedom and Privacy, Montréal, Canada, 1 - 4 May 2007, <http://www-polytic.lip6.fr/article.php3?id_article=174>

The presence of illegal and harmful content on the Internet has led governments and private institutions to take measures using different types of Internet content regulation. Government regulation, self-regulation and co-regulation are amongst the various options for restricting the rights to freedom of expression on the Internet. However, these restrictions have the potential to damage the basis for the freedom of expression. Therefore, taking into account the principles which are rooted in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), European Union (EU) institutions have developed different approaches in order to protect freedom of expression on the Internet.

The Internet has been a catalyst in establishing a democratic society in Turkey. Thanks to the Internet, even offensive or shocking ideas may be debated, regardless of any frontiers. Considering the history of anti-democratic intervention in Turkey, in recent years the Internet has become an important tool for establishing fertile grounds for freedom of expression. However, some exaggerated concerns have obliged the Turkish government to introduce certain regulations in order to deal with undesirable Internet content.[7] As a result of these regulations, some websites such as YouTube and Geocities have been blocked.

Turkey, as a candidate country for EU membership, is required to ensure that its laws are compatible with the Internet content regulatory approaches of the EU.[8] Moreover, Turkish legislation and applications regarding Internet content are subject to the principles of freedom of expression established by the European Court of Human Rights (ECtHR).[9] However, both the relevant regulations and their application in Turkey have been criticised as being deficient in comparison to European approaches and ECtHR principles regarding the freedom of expression.

---

[7] For instance, the media exaggerated claims that on-line child pornography had become widespread in Turkey. However, police indicated that Turkish children were not used in pornographic productions, by reference to Interpol's database.

[8] Y. Akdeniz, 'Internet Governance, and Freedom in Turkey', 2003, p.7, <http://www.cyber-rights.org/documents/osce_turkey_paper.pdf>

[9] *Supra*, n. 8, p. 2

In this context, this dissertation aims to assess Turkish case within the framework of the principles of the freedom of expression. Following this introductory chapter, the second chapter will elaborate on the various types of Internet content regulation, as well as the European approach to Internet content regulation. In the third chapter, the relationship between freedom of expression and Internet content regulation will be analysed in the light of Article 10 of the ECHR and ECtHR case-law. In the fourth chapter, the regulatory framework for Internet content and access-blocking applications in Turkey are assessed within the context of the principles of freedom of expression. Finally, some remarks and proposals will be made in the concluding chapter.

2. INTERNET CONTENT REGULATION

2.1 Types of Internet Content Regulation

The need for Internet content regulation has paved the way for the introduction of regulatory tools, such as government regulation, self-regulation and co-regulation, so as to deal with undesirable Internet content.

2.1.1 Government Regulation

Governments have traditionally been responsible for laying down rules in order to determine and expose illegal activities.[10] As government is considered as 'a virtual monopoly on the market for regulation in the physical world',[11] legislative regulation has been the tool most prevalently used by governments, so as to restrict the circulation of harmful and illegal Internet content. However, it can be said that the issue of government intervention has led to divergent arguments between commentators.

One of the most controversial issues regards the role of government in the cyberspace. On one hand, Geist asserts that governments do not have the authority to regulate Internet content due to the borderless features of Internet.[12] Perry Barlow declares that governments have no sovereignty in cyberspace. He also alleges that conventional legal concepts, such as property, expression and identity, do not have any field of application in cyberspace. He asserts that problems in cyberspace should be solved by their own instruments.[13] Post and Johnson consider cyberspace to be a distinct place, where the Internet users can create their own rules by means of self-regulation tools.[14]

---

[10] *Supra*, n. 1, p. 45
[11] T. B. Nachbar, 'Paradox and Structure: Relying on Government Regulation to Preserve the Internet's Unregulated Character', 85 Minn. L. Rev. 215, November 2000, p.260
[12] M. Geist, 'Cyberlaw 2.0', 44 B.C. L. Rev 323, March 2003, p.331
[13] J. P. Barlow, 'A Declaration of the Independence of Cyberspace', Davos, Switzerland, 8 February 1996, <http://www.lafraze.net/nbernard/misc/Declaration-Final.html>
[14] D. Post, D. R. Johnson, 'Law and Borders -The Rise of Law in Cyberspace', 48 Stan. L. Rev. 1995-1996, p.1367

On the other hand, Tambini et al. claim that the idea of an Internet without regulation is not realistic.[15] They indicate that rules are essential for freedom, and freedom of expression on the Internet does not refer to the absence of rules.[16] According to them, the main point of focus should be whether rules are 'democratically set at the necessary minimum, procedurally fair, accountable and in the public interest'.[17] Furthermore, Schönberger asserts that government reaction is indispensable, since it provides democratic legitimacy and direct enforceability.[18] Schultz claims that it is impossible for governments to abdicate their duty 'to protect national interest and enforce national values'.[19]

The European Internet Co-Regulation Network (EICN),[20] taking into account common social values, considers the Internet to be a social space which needs to be regulated by governments. It is claimed that the future of the Internet would be in danger if the social aspect of this space were to be disregarded.[21] Moreover, considering the borderless features of the Internet, Geist quotes Lessig, stating that a government may lose its sovereignty if it does not regulate Internet content.[22] Goldsmith and Wu highlight the importance of developing new strategies for regulating the Internet; however, they suggest that these should not decrease the vital role of territorial governments.[23] They place an emphasis on the role of territorial governments,[24] stating that the Internet requires government control.[25]

---

[15] D. Tambini, D. Leonardi, C. Marsden, *Codifying Cyberspace: Communications self-regulation in the age of Internet convergence*, Routledge, 2008, p.294
[16] *Supra*, n. 15, p. 296
[17] *Supra*, n. 15, p. 295
[18] V. M. Schönberger, 'The Shape of Governance: Analyzing the World of Internet Regulation', Virginia Journal of International Law, Spring 2003, p.612
[19] T. Schultz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface', The European Journal of International Law, Vol. 19 no.4, EJIL, 2008, p.839
[20] The EICN, supported by the Commission, is an international initiative which aims to establish co-operation on rights and usage issues between all players on the Internet.
[21] EICN, 'Report on Internet Governance', July 2005, p.5, <http://www.clubofamsterdam.com/contentarticles/28%20Governance/Report%20on%20Internet%20Governance.pdf>
[22] *Supra*, n. 12, p. 328
[23] J. Goldsmith, T. Wu, *Who Controls the Internet? Illusions of Borderless World,* Oxford University Press, 2006, p.180
[24] *Supra*, n. 23, p. 181
[25] *Supra*, n. 23, p. 142

However, Mueller characterizes Goldsmith and Wu's approach as 'cyber-conservatism'. He criticises them because of their resistance to change, and he claims that their approach suffers from a lack of institutional creativity. In order to disprove their approach, he demonstrates that the required governance for the Internet can be achieved by means of an international body, Internet Corporation for Assigned Names and Numbers (ICANN), instead of that of traditional territorial governments.[26]

Another contradictory issue is the applicability of traditional media regulations to the Internet. Koomen emphasizes that the regulatory approach to traditional media cannot be transferred to the Internet, due to a lack of central control, and ease of access to Internet content.[27] However, contrary to Koomen, Capitanchik and Whine state that the laws which are already in place for traditional media should also be applied to the Internet.[28] Fagin believes that it is inevitable and legitimate to apply national regulations to cyberspace, since the Internet is convenient to local regulation and nation-specific law.[29] It is submitted that, having regard to its specific features, the Internet requires different rules to traditional media.

The technical and operational deficiencies of government regulation have also been a target for criticism. Some technical characteristics of the Internet pose special challenges to government regulation. For instance, even if a government removes published content from a server, there is almost nothing to prevent it from being copied to other servers in other jurisdictions.[30]

---

[26] M. L. Mueller, 'The New Cyber-Conservatism: Goldsmith/Wu and the Premature Triumphalism of the Territorial Nation-State: A review of Goldsmith and Wu's Who Controls the Internet? Illusions of a Borderless World', p.4, <http://internetgovernance.org/pdf/MM-goldsmithWu.pdf>

[27] K. Koomen, 'Emerging Trends: Content Regulation in Australia and Some International Developments', AIC Conference, Sydney, 21-22 May 1997, p.4, <http://www.acma.gov.au/webwr/aba/newspubs/speeches/documents/kkaic_97.pdf>

[28] *Supra*, n. 5

[29] M. Fagin, 'Regulating Speech across Borders: Technology vs. Values', 9 Mich. Telecomm. Tech. L. Rev. 395, p.403

[30] European Commission, 'Communication on Illegal and Harmful Content on the Internet', COM(96) 487 final, Brussels, 16 October 1996, p.12, <http://aei.pitt.edu/5895/01/001527_1.pdf>

A new concept of 'regulatory arbitrage' has been suggested; this means that the Internet's decentralised mechanism enables users to abstain from national regulations, so as to benefit from foreign regulatory systems. It is claimed that this situation promotes freedom of expression and 'reduces the policy flexibility of nations by making certain types of domestic rules difficult to enforce'.[31] According to Hanley, despite huge efforts towards, and subsidies for, government regulation, it can be circumvented by 'merely contacting an overseas Internet Service Provider (ISP)'.[32]

Akdeniz, besides acknowledging the virtues of government regulation such as legitimacy and applicability,[33] argues that governments are ineffective and inadequate in addressing problems associated with the Internet. He supports his argument by claiming that governments inherently face problems in adapting to changes in technology.[34] Moreover, he states that it is difficult to fulfil procedures with regard to enacting and amending legislation. According to him, the broad discretionary powers given to legislators leads to arbitrariness in applying legislation. In addition, legislation is expensive, leading to a high cost in relation to the interpretation, application, and enforcement of these laws.[35] Akdeniz suggests alternatives to government regulation for developing Internet related policies.[36]

The International Chamber of Commerce (ICC)[37] states that over-regulation of Internet content leads to legal and operational obstacles for business, and creates a chilling effect on promoting economic development. For this reason, it is proposed that governments should refrain from the over-regulation of Internet content. Moreover, it is claimed that government regulations, which

[31] D. Dunne, 'Governance of Controversial Internet Content in the European Union', Minor Dissertation, University College Dublin, 1997, p.4, <http://www.danieldunne.com/dunnethesis.pdf>
[32] S. M. Hanley, 'International Internet Regulation: A Multinational Approach', 16 J. Marshall J. Computer & Info. L. 997, 1998, p.1022
[33] Y. Akdeniz, 'Internet Governance: Towards the Modernization of Policy Making Process in Turkey', Papatya, October 2003, p.24, <http://www.cyber-rights.org/documents/beyaz_kitap_english.pdf>
[34] *Supra*, n. 33, p. 2
[35] *Supra*, n. 33, p. 25
[36] *Supra*, n. 33, p. 2
[37] ICC is an organisation which functions in various fields such as arbitration and dispute resolution, business self-regulation, fighting corruption or dealing with commercial crime.

potentially place 'additional costs and burdens on business', would damage the ground for competition.[38]

To sum up, the Internet is not a lawless place, and the inherent freedom of the Internet should not be misused in terms of illegal and harmful content. It is submitted that commentators such as Schönberger, Tambini et al. are correct in stating that an approach which excludes government from cyberspace does not reflect the realities. Moreover, the importance of government intervention should not be ignored, since it provides democratic legitimacy and direct enforceability. On the other hand, Akdeniz and the ICC are correct in noting that government regulation suffers from technical and operational deficiencies. In order to tackle with these shortcomings, it is argued that government regulations should be supported through alternative means, such as self-regulation or co-regulation.

2.1.2 Self-Regulation

Self-regulation is another method of regulating Internet content;[39] it provides non-governmental organizations with the opportunity to create and implement rules for themselves,[40] and for others who recognise their authority.[41] The Office of Communications (Ofcom) describes self-regulation as a solution carried out by industry without government intervention.[42] In contrast to the ICC, which considers self-regulatory mechanisms to be compelling alternatives to legislation,[43] Baldwin and Cave claim that a self-regulatory system creates informal and voluntary solutions.[44]

---

[38] ICC, 'The Impact of Internet Content Regulation', Commission on E-Business, IT and Telecoms, 18 November 2002, <http://iccwbo.org/id510/index.html>
[39] *Supra*, n. 4
[40] J. Cave, C. Marsden, '*Quis custodiet ipsos custodies* in the Internet: Self-regulation as a Threat and a Promise', 28 September 2008, p.7, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1366723>
[41] J. Black, 'Constitutionalising Self-Regulation', 59 Mod. L. Rev. 24, 1996, p. 27
[42] Ofcom, 'Identifying Appropriate Regulatory Solutions: Principles for Analysing Self- and Co-Regulation', 10 December 2008, p.8, <http://www.ofcom.org.uk/consult/condocs/coregulation/statement/statement.pdf>
[43] *Supra*, n. 38
[44] R. Baldwin, M. Cave, *Understanding Regulation: Theory, Strategy, and Practice*, Oxford University Press, 1999, p.127

2.1.2.1 Self-Regulation Tools

Internet content filtering, rating and hot-lines are the most common tools utilised in self-regulation.

Internet content filtering is performed using software that compares all content with filtering criteria prior to that content being viewed on a computer.[45] There are basically four categories of Internet content filtering: the first two categories are 'blacklisting' and 'white listing', which are based on maintained lists of websites; the third category relates to software that analyses content by blocking certain phrases as they are confronted, or by blocking all content posted on a particular web address, if it includes certain phrases.[46]

The fourth category consists of ratings-based filtering, whereby Internet users can search only rated content.[47] As a response to Internet legislation in the US, the World Wide Web Consortium (W3C) developed a ratings system for the Internet, which was called the 'Platform for Internet Content Selection' (PICS).[48] PICS is a technical standard, which is used for limiting access to adult content by children, by labelling Internet sites with 'value neutral' tags.[49] PICS aims to rate on-line content in nine groups, including 'sex, violence, and profanity on a scale of one to four'.[50] Each user is required to rate the uploaded content, and third parties decide whether or not to view the content according to these ratings. In order to view the site, it should have a PICS label, and should fall within the data set by families on their computers.[51] The purpose of PICS is to engineer Internet sites, and to provide control of content at the computer, instead of by ISP.[52]

---

[45] *Supra*, n. 11, p. 223
[46] *Supra*, n. 11, p. 224
[47] R. F. Jørgensen, *Human Rights in the Global Information Society*, Cambridge, Mass.: MIT Press, 2006, p.63
[48] J. Westfall, 'Internet Blocking', Santa Clara University, <http://www.scu.edu/ethics/publications/submitted/westfall/blocking.html>
[49] *Supra*, n. 31, p. 50
[50] *Supra*, n. 32, p. 1007
[51] *Supra*, n. 31, p. 50
[52] *Supra*, n. 15, p. 3

In addition to filtering and rating, the 'hot-line' is another self-regulatory tool.[53] With this system, users make complaints about Internet content to hot-lines.[54] The hot-line operators evaluate these reports, and determine whether the content is illegal or not. If the hot-line operators consider the content to be illegal, they notify the ISPs to request that they remove this content from their servers.[55]

An example of a national hot-line is the Internet Watch Foundation (IWF), which operates in the UK. Internet users are encouraged to report potentially illegal content, such as child pornography, criminally obscene content and racial hatred content, to the IWF. A special team called the 'Internet Content Analysts' is authorised to evaluate relevant Internet content in accordance with UK law.[56] If the IWF determines that the content in question is illegal in terms of UK legislation, it notifies the relevant UK ISP to remove the content. However, if the hosting ISP is situated outside the UK, the IWF is required to get in touch with that ISP wherever it is based.[57] In addition, the IWF is responsible for developing ratings systems, so as to protect minors from harmful content.[58]

2.1.2.2 Arguments Regarding Self-Regulation

The proponents of self-regulation generally allege that the architecture of the Internet, and the deficiencies of government regulation, have given rise to preferences for self-regulatory mechanisms rather than government

[53] Hot-lines may be established within an ISP, or a private body or government body may function as a hot-line.
[54] *Supra*, n. 1, p. 37
[55] Y. Akdeniz, 'Stocktaking on Efforts to Combat Racism on the Internet', High Level Seminar on Racism and the Internet, Geneva, January 2006, p.35, <http://www.cyber-rights.org/reports/ya_un_paper_int_06.pdf>
[56] The Internet Watch Foundation, 'IWF Facilitation of the Blocking Initiative', <http://www.iwf.org.uk/public/page.148.437.htm>
[57] Article19.org, 'Background Paper on Freedom of Expression and Internet Regulation for the International Seminar on Promoting Freedom of Expression with the Three Specialised International Mandates', London, United Kingdom, 19 - 20 November 2001, p.10, <http://www.article19.org/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf>
[58] CP Walker, Y. Akdeniz, 'The Governance of the Internet in Europe with Special Reference to Illegal and Harmful Content', Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet, 1998, p.5

regulation. For instance, Walker indicates that he sees self-regulation as an instrument which discards with clumsy intervention by government.[59]

Brown draws attention to the flexibility of self-regulatory tools i.e. filtering technologies whereby new fields of undesired content can be covered.[60] Agreeing with Brown, Akdeniz believes that self-regulation is more enforceable than government regulation, as it is more responsive to the changing needs of the Internet. He describes self-regulation as a cost-effective tool against illegal and harmful content, as its costs can be passed on the industry involved. Especially in relation to the fight against harmful content, he claims that self-regulation provides subjective solutions for users.[61] Ofcom states that self-regulation provides the industry with 'a sense of responsibility' in dealing with Internet content issues.[62] Baldwin and Cave emphasize that self-regulatory bodies benefit from high levels of expertise and technical knowledge in comparison with government regulation.[63]

On the other hand, Edelstein claims that the diversity of Internet users makes it almost impossible to agree on enforceable standards and rules.[64] Furthermore, in spite of being applauded as the most useful and convenient solution by the European Commission,[65] self-regulatory tools, such as PICS, leads to an accountability deficit, since ratings are drawn up by private bodies instead of government.[66] Weinberg refers to the difficulty of categorizing all Internet sites, and claims that ratings systems such as PICS conduce to high costs, aside from any benefits.[67] Taking into account the enormous amount of information circulating across the Internet, and the time required to filter all

[59] C. Walker, 'Cyber-Contempt: Fair Trials and the Internet', Yearbook of Media and Entertainment Law, 1997, p.537
[60] I. Brown, 'Internet Censorship: Be Careful What You Ask for, forthcoming', 2008, p.8, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1026597>
[61] *Supra*, n. 33, p. 26
[62] *Supra*, n. 42, p. 8
[63] *Supra*, n. 44, p. 126
[64] J. I. Edelstein, 'Anonymity and International Law Enforcement in Cyberspace', 7 Fordham Intellectual Property, Media & Entertainment Law Journal, 1996, p.284
[65] *Supra*, n. 31, p. 49-50
[66] *Supra*, n. 31, p. 54
[67] J. Weinberg, 'Rating the Net', Hastings Communication and Entertainment Law Journal 453, 1997, <http://faculty.law.wayne.edu/Weinberg/rating.htm>

this information, it is argued that filtering software such as PICS suggests delusive solutions.[68]

Moreover, Walker and Akdeniz believe that self-regulatory solutions give rise to discretionary censorship.[69] It is also indicated that self-regulatory bodies do not have adequate powers to sanction the relevant parties in cases of infringement of self-regulatory rules.[70] Kiškis and Petrauskas assert that self-regulation has a deficiency regarding the enforceability of rules by actors in the self-regulation industry.[71]

Tambini et al. acknowledge self-regulation as an efficient solution for protecting fundamental rights, such as freedom of expression.[72] However, Marzouki argues that Internet self-regulation has the potential to infringe 'guarantee-rights', which are considered to be fundamental components of the rule of law. Within the context of self-regulatory measures, ISPs have the right to 'remove content they host, or block content they give access to'. These removing or blocking applications are alleged to be unlawful, because they are not based on any court decisions. She asserts that this situation is tantamount to a breach of the right of access to a court, and 'the principle of no punishment without law'. That is why, in addition to indicating the necessity of court decisions for any content removal or blocking applications, she also proposes limiting the role of ISPs or hot-lines in enforcing judicial orders for content removal.[73]

Akdeniz, agreeing with Marzouki, asserts that determination of illegality should 'remain as a matter for the courts of law rather than hotline operators'.[74] According to Akdeniz and Altıparmak, hot-lines or ISPs are not qualified to

[68] *Supra*, n. 32, p. 1008
[69] *Supra*, n. 58, p. 11
[70] M. E. Price, S. G. Verhulst, *Self-regulation and the Internet*, The Hague: Kluwer Law International, 2005, p.10
[71] *Supra*, n. 4
[72] *Supra*, n. 15, p. 291
[73] M. Marzouki, 'Combating Racism on the Internet while Upholding International Human Rights Standards', 19 January 2006, <http://www-polytic.lip6.fr/imp-article.php3?id_article=127>
[74] *Supra*, n. 55, p. 35

judge the harmfulness or illegality of Internet content.[75] Akdeniz also argues that ISPs and hot-lines generally do not provide any opportunity for banned content providers to appeal against their decisions.[76]

Furthermore, in its very recent decision, the French Constitutional Council held that the power to 'limit the exercise by any person of one's right to express oneself and freely communicate' can only be allocated to a judge, and not to an administrative or private body. In other words, the Council states that Internet users should only face sanctions imposed by a court.[77]

Another challenging issue for self-regulation is the 'free-rider phenomenon', which means that 'some actors expend significant resources on the development, monitoring and implementation of codes and standards, while others simply profit from their existence or ignore them altogether'.[78] Akdeniz argues that self-regulating arrangements may distort the ground for competition, by recognising the commercial advantage for a particular group, or by prohibiting new entrants to the market.[79]

In practice, ISPs or hot-lines have the right to remove or block content without any judicial scrutiny. In agreement with Akdeniz and Marzouki, it is submitted that the authority of determining illegality should belong solely to the courts, and not hot-lines or ISPs, since they are not legally entitled to judge the illegality of Internet content. Moreover, content providers whose material has been banned should be given legal means for appealing against the decisions of ISPs or hot-lines.

To sum up, self-regulation has emerged in response to the shortcomings of government regulation. Flexibility, cost-efficiency, providing subjective

[75] Y. Akdeniz, K. Altıparmak, 'Internet: Restricted Access A Critical Assessment of Internet Content Regulation and Censorship in Turkey', November 2008, p.63, <http://www.cyber-rights.org/reports/internet_restricted_colour.pdf>
[76] Y. Akdeniz, 'The Regulation of Pornography and Child Pornography on the Internet', 28 February 1997, p.32, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=41684>
[77] EDRI-gram, 'The French Constitutional Council censures the 3 strikes law', Number 7.12, 17 June 2009, <http://www.edri.org/book/export/html/1967>
[78] *Supra*, n. 1, p. 22
[79] *Supra*, n. 33, p. 27

solutions and a sense of responsibility for users, as well as the high levels of expertise provided by self-regulatory bodies, are some of the features of self-regulation. However, self-regulatory applications have demonstrated that self-regulation also suffers from shortcomings. Difficulty on agreeing on enforceable standards and rules, the issue of the free-rider phenomenon, the possibly chilling effect on competition, and the high cost of rating websites are weaknesses of self-regulation. In addition to these deficiencies, the inadequacies of imposing sanctions for infringements and problems regarding enforceability of rules reveal that self-regulation should be reinforced through government regulation.

2.1.3 Co-Regulation

Government regulation constituted the first stage of regulating the Internet. However, 'the technical, fast-changing and global nature of the Internet' revealed the ineffectiveness of government regulation.[80] For this reason, the private sector has developed various self-regulation mechanisms which operate without government intervention. Some issues, such as a lack of enforceability in applying self-regulatory rules, have demonstrated that the self-regulation stage should be supported through government regulation. In this context, the appearance of a new approach to rule-making, called co-regulation has been developed in order to enable collaboration between the government and the industry in a more balanced, flexible, and transparent manner.[81]

EC Commissioner Reding places particular emphasis on a co-regulatory system, and defines this system as,

> …one where public authorities accept that the protection of societal values can be left to self-regulatory mechanisms and codes of conduct,

[80] *Supra*, n. 1, p. 45
[81] *Supra*, n. 21, p. 3

but where they reserve the right to step in in case that self-regulation should prove to be inefficient.[82]

Akdeniz considers government intervention to play an important role in dealing with illegal content. However, he suggests that ISPs may be efficient in preventing the circulation of illegal content by means of self-regulation tools in accordance with government regulation.[83] Accordingly, he implies that co-operation between government and industry may be conducive to accomplishing government's aims. He believes that this sort of co-operation paves the way for creating co-regulatory initiatives, as an alternative to government regulation in dealing with harmful content. The aim of co-regulation is to marry the enforceability of government regulation with the flexibility of self-regulation. According to Akdeniz, co-regulatory solutions are flexible because they are easily adjustable to the new needs or goals of a certain government. Furthermore, co-regulation enables governments to enforce 'more formal regulation' in cases where the industry fails to respond effectively in dealing with undesirable content. Another advantage of co-regulation is its lower administration costs for the government.[84]

There are mainly two forms of practice regarding co-regulation. The first is 'regulated self-regulation', in which the industry takes measures to regulate it, and governments validate these measures. In this model, government works closely with private sector so as to control self-regulatory tools.[85]

According to the second approach, public and private actors share responsibility for Internet content regulation, by forming a 'multi-stakeholder partnership'.[86] The EICN suggests that there should be real co-operation between stakeholders, rather than a bilateral dialogue between government and other interested parties.[87] This approach gives rise to transparent

[82] E. Lievens, 'Harmful New Media Content: The Latest Regulatory Trends', Communications Law, 2006, p.6
[83] *Supra*, n. 55, p. 33
[84] *Supra*, n. 33, p. 29
[85] *Supra*, n. 21, p. 4
[86] *Ibid*, p. 4
[87] *Supra*, n. 21, p. 6

discussions between the private and public sectors so as to develop common solutions. This form of governance requires parties to contribute to the rules governing them.[88] Cave and Marsden imply that this form of co-regulation is more flexible and adaptable in comparison with the 'regulated self-regulation' approach.[89]

The second co-regulation approach introduces two different co-regulatory mechanisms: government-centred and co-regulatory body mechanisms. Tambini et al. support a government-centred co-regulation approach. They state that, in contrast to self-regulation, which excludes government, government should have a co-operative role in co-regulation by developing rules and regulations along with other stakeholders.[90] They regard co-regulation as the instrument to strike the right balance between government regulation and self-regulation.[91] They believe that the freedom of expression concerns arising from self-regulation can be eliminated through this type of co-regulation.[92]

Lievens proposes some criteria for co-regulatory body mechanisms. She states that government should devolve its discretionary powers to a non-government regulatory mechanism. She asserts that the main aim of this system should be to accomplish 'public policy goals targeted at social processes'. Furthermore, she points out the importance of establishing a legal link between governmental and non-governmental regulatory systems.[93] Ofcom deems it vital to describe the responsibilities of co-regulatory bodies and government respectively. It is proposed that co-regulatory bodies should be independent from government. In order to establish a clear and transparent basis for co-regulation, Ofcom suggests that a document be drafted which outlines the terms of reference designating the responsibilities of each party.[94]

[88] *Supra*, n. 21, p. 4
[89] *Supra*, n. 40, p. 35
[90] *Supra*, n. 15, p. 4
[91] *Supra*, n. 15, p. 43
[92] *Supra*, n. 15, p. 301
[93] *Supra*, n. 82, p. 6
[94] *Supra*, n. 42, p. 24

In this context, it is obvious that co-regulation strikes the right balance between government regulation and self-regulation, by means of merging the enforceability of government regulation with the flexibility of self-regulation. Co-regulation not only highlights the positive aspects of government regulation and self-regulation, but also controls the negative aspects. Having regard to the importance of co-operation in dealing with issues on Internet content, it is argued that the co-regulation approach with 'multi-stakeholder partnership' is more convenient than 'regulated self-regulation'. It is further argued that Ofcom is correct in its stance that the success of co-regulation mechanisms with 'multi-stakeholder partnerships' depends on a clear differentiation of the responsibilities of each party.

2.2 European Approach to Internet Content Regulation

There are significant efforts being made to combat against illegal and harmful content on the Internet at European levels. The main standpoint of the European approach has been to consider 'what is illegal off-line is illegal on-line',[95] to promote self-regulation tools such as filtering and rating systems.[96]

The main issues with regard to Internet content regulation will be examined within the framework of EU and Council of Europe standards.

2.2.1 Distinction between Harmful and Illegal Content

The European point of view regarding Internet content regulation requires different legal and technological responses in relation to illegal and harmful uses of the Internet.[97]

[95] European Commission, 'European Union Approach to Illegal and Harmful Content on the Internet', p.1, <http://www.copacommission.org/meetings/hearing3/eu.test.pdf>
[96] B. Niere, 'European Commission: Communication on illegal and harmful content on the Internet and Green Paper on the protection of minors and human dignity', IRIS Legal Observations of the European Audiovisual Observatory, IRIS 1996-10:4/3, p.1
[97] First Report of Working Group, 'Illegal and Harmful Use of the Internet', p.2, <http://ec.europa.eu/avpolicy/docs/reg/minors/useinternet1streport_ie.pdf>,

Once illegal content has been criminalized by national laws, access by anyone, regardless of that person's age, is prohibited. This type of content constitutes 'a general category of material that violates human dignity, primarily consisting of child pornography, extreme gratuitous violence and incitement to racial and other hatred, discrimination, and violence'.[98]

The EU focuses mainly on child pornography, terrorism, racism and xenophobia with regard to illegal content. Because of its special significance, combating child pornography is prioritized by the EU through a Council Framework decision.[99] Furthermore, the fight against racism and xenophobia are considered to be issues which should be dealt with separately. For this reason, the EU has started work on a Framework Decision which sets out effective criminal penalties dealing with these issues.[100] In this respect, the Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services[101] focuses on specific types of illegal content such as anti-Semitic and racist material.[102]

Despite the fact that governments are responsible for fighting against illegal content, and that the determination of illegality is generally made by means of judicial procedures,[103] according to the EU approach, the industry and users are also considered to be part of this fight through establishing and running hot-lines for reporting illegal content. The Safer Internet Action Plan (SIAP)[104] draws attention to the establishment of a European network of hot-lines, which

---

[98] D. Oswell, 'The Dark Side of Cyberspace: Internet Content Regulation and Child Protection', Convergence: The International Journal of Research into New Media Technologies, p.46, <http://con.sagepub.com/cgi/reprint/5/4/42>

[99] The Council of the European Union, 'Council Framework Decision of on Combating the Sexual Exploitation of Children and Child Pornography', 10748/03, Brussels, 29 July 2003, <http://register.consilium.eu.int/pdf/en/03/st10/st10748en03.pdf>

[100] *Supra*, n. 75 , p. 66

[101] European Commission, 'Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services', COM(96) 483, Brussels, 16 October 1996, <http://aei.pitt.edu/1163/01/minors_info_soc_gp_COM_96_483.pdf>

[102] I. Walden, J. Angel, *Telecommunications Law and Regulation*, OUP, 2nd Edition, 2005, p. 417

[103] *Supra*, n. 97, p. 2

[104] European Parliament and Council of the European Union, 'Decision on Adopting a Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks', No. 276/1999/EC, OJ L 33, 25 January 1999

enable users to report illegal content to both law-enforcement agencies and industry.[105] The International Association of Internet Hot-lines (INHOPE), which was formed by non-governmental groups, tries to achieve Internet safety by supporting national hot-lines in their fight against illegal content.[106] Since it is partly funded by the European Commission, INHOPE is not considered a purely self-regulatory body.[107]

Harmful content is considered to be material which has the potential to damage the physical and mental development of children. In contrast to illegal content, harmful content is considered legal,[108] and it may be consumed freely by adults.[109] The scope of harmful content is a controversial issue at European level. Walker and Akdeniz state that even though there is a common understanding that 'harmful content needs to be treated differently from illegal content', there is no clarity in EU regulations on the scope of the term 'harmful'.[110] The European Commission Communication on Illegal and Harmful Content on the Internet (Communication)[111] appears to frame harmful content as being content harmful to the development of minors, but which should not be legally prohibited. However, it is asserted that the Communication includes a broader definition for harmful content which includes expressing political opinions, religious beliefs or views on racial matters.[112] Despite the contradiction concerning its definition, it is argued here that the scope of harmful content should be described as being that which is harmful to children.

In the Communication, issues related to Internet content have been separated into 'illegal' and 'harmful' content. The Communication criticises the merging

[105] *Supra*, n. 95, p. 2
[106] INHOPE, 'The International Association of Internet Hotlines, Towards Online Safety: Taking Action Today, Ready for Tomorrow', Third Report, 2006, p.8, <https://www.inhope.org/system/files/inhope_report_2006.pdf>
[107] C. Marsden, S. Simmons, I. Brown, L. Woods, A. Peake, N. Robinson, S. Hoorens, L. Klautzer, 'Options for and Effectiveness of Internet Self- and Co-Regulation Phase 2: Case Study Report', 15 January 2008, <http://ssrn.com/abstract=1281374>
[108] C. Canbay, 'Internet Content Regulation: Comparative Analysis of Turkish and English Legislation', Dissertation, University of Essex, 2007, p.13
[109] *Supra*, n. 98, p. 46
[110] *Supra*, n. 58, p. 9
[111] *Supra*, n. 30, p. 10
[112] *Supra*, n. 31, p. 33

of separate issues such as 'children accessing pornographic content for adults, and adults accessing pornography about children'. Within the scope of the Internet Bill of Rights, Peers emphasises the importance of striking a balance between the freedom of expression of adults, and the protection of children against harmful content.[113] Oswell claims that the fight against illegal content is broadly supported, whereas harmful content requires more localised mechanisms of governance.[114]

Accordingly, it is asserted that conventional methods of censorship are ineffective, and that the responsibility for creating a safe Internet must be shared by different parties, such as parents or educators.[115] That is why parental controls and education are designated as the main tools for families to deal with harmful content. In this context, the Recommendation on Protection of Minors and Human Dignity[116] promotes the establishment of national self-regulatory mechanisms, such as codes of conduct, and suitable rating and filtering systems.[117] The filtering model provides for 'downstream control' by parents in order to protect their children from harmful content. It emphasizes individual responsibility, rather than 'upstream censorship' by government.

This type of content regulation receives strong support from the industry, since it is sensitive to cultural and national distinctions between countries. As each country may have a different understanding of what constitutes permissible content for minors, it is important to apply appropriate ethical standards in these countries, so as to establish suitable rules against offensive content.[118] At EU level, Member States are considered to have the

[113] S. Peers, 'Strengthening Security and Fundamental Freedoms on the Internet - An EU Policy on the Fight against Cyber Crime', p.28, <http://www.europarl.europa.eu/activities/committees/studies/download.do?file=24233>
[114] *Supra*, n. 98, p. 47
[115] *Supra*, n. 97, p. 2
[116] European Parliament and Council of the European Union, 'Recommendation on the Protection of Minors and Human Dignity and on the Right of Reply in Relation to the Competitiveness of the European Audiovisual and On-line Information Services Industry', (2006/952/EC), 20 December 2006, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:378:0072:0077:EN:PDF>
[117] *Supra*, n. 95, p. 2
[118] *Supra*, n. 31, p. 33

necessary authority to protect minors within the framework of their own ethical values.[119] Therefore, as a pragmatic solution to harmful content, the filtering system provides 'end user autonomy, respect for freedom of expression, a diversity of beliefs and values, transparency, respect for privacy and inter-operability and compatibility'.[120]

In summary, according to the European approach, undesirable Internet content should be separated into two groups: illegal or harmful content. It is submitted that government regulations and self-regulation tools should go hand-in-hand in the fight against illegal content.

However, harmful content requires an entirely different regulatory approach in comparison to illegal content, since harmful content is legal for adults. Due to a divergence of ethical values, European countries are allowed to protect their minors within the framework of their own values. In this respect, as the most suitable solution for end-user autonomy, respect for freedom of expression and a diversity of values, parents and users should be encouraged to use self-regulatory tools in dealing with harmful content. Whilst protecting minors from harmful content, it is also vital to protect the freedom of expression of adults. Thus, it is necessary for governments to refrain from regulating harmful content, since it affects adults' rights to access adult pornography. Filtering technologies that block access to legitimate content for adults also give rise to infringements of freedom of expression. Therefore, self-regulatory tools should be applied, so that the right to access legitimate content is not prohibited.

2.2.2 Trend towards Self-Regulation or Co-Regulation

Self-regulation and co-regulation have been considered as alternatives to government regulation at European level.

[119] *Supra*, n. 75, p. 71
[120] *Supra*, n. 1, p. 30

The Audiovisual Media Services Directive,[121] which also covers novel forms of delivery modes such as the Internet in addition to audiovisual services,[122] is a significant reference for co-regulation on the Internet. According to Recital 36 of the Directive, co-regulation is defined as 'a legal link between self-regulation and the national legislator in accordance with the legal traditions of the Member States'. It is held that where self-regulatory tools fail to be applied, co-regulation should pave the way for government intervention.[123]

The Communication promotes the use of self-regulation tools, and emphasizes the significance of establishing a European network of ISPs. This regulation encourages the industry to co-ordinate different approaches, and encourages users to make a contribution to self-regulatory mechanisms.[124] User-based software is regarded as an efficient tool for enabling parents to protect their children from harmful content.[125]

The Inter-Institutional Agreement on Better Law-Making, which was concluded by the European Parliament, the Council and the Commission, aims to frame the scope of co-regulation and self-regulation.[126] The Council of Europe's Committee of Ministers has adopted the Declaration on Freedom of Communication on the Internet[127], which proposes that Member States promote self-regulation or co-regulation in relation to harmful or illegal content on the Internet.

---

[121] Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 Amending Council Directive 89/552/EEC on the Coordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States Concerning the Pursuit of Television Broadcasting Activities, 18 December 2007

[122] P. Valcke, D. Stevens, E. Lievens, E. Werkers, 'Audiovisual Media Services in the EU Next Generation Approach or Old Wine in New Barrels?', p.107, <http://www.law.kuleuven.be/icri/publications/1149CS71_VALCKE_et_al.pdf?where=>

[123] *Supra*, n. 122, p. 109

[124] *Supra*, n. 30, p. 14

[125] *Supra*, n. 30, p. 23

[126] European Commission, 'Communication from the Commission to the Council and the European Parliament, Better Regulation for Growth and Jobs in the European Union', Com(2005) 97 Final, Brussels, 16 March 2005, <http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0097en01.pdf>

[127] Council of Europe, 'Declaration on Freedom of Communication on the Internet', 28 May 2003, <https://wcd.coe.int/ViewDoc.jsp?id=37031>

SIAP is another document which fosters self-regulation for the purpose of decreasing the volume of illegal and harmful content on the Internet. SIAP encourages the industry to establish filtering and ratings systems, which enable parents to identify appropriate content for children.[128] SIAP also stresses the importance of raising users' awareness within the context of selecting the proper control tools.[129] However, the Economic and Social Committee of the European Commission has found SIAP 'impracticable' for its measures regarding rating and classifying all content on the Internet. Furthermore, the Committee suggests that SIAP should focus on dealing with illegal content, instead of harmful content.[130]

To conclude, it is pertinent to note that co-regulation and self-regulation have been encouraged through various European regulations. A tendency to shift from government regulation to self-regulation or co-regulation can be seen at European level.

2.2.3 European Stance on Blocking Applications

Regulations at different levels reveal the fact that the European approach stands aloof from blocking applications.

According to Recommendation CM/Rec (2008) of the Committee of Ministers,[131] and the Declaration adopted by the Council of Europe Committee of Ministers,[132] Member States are not permitted to apply general blocking to information and other communication on the Internet without considering the boundaries set down in Article 10(2) of the ECHR. The Recommendation also

[128] T. Cabe, 'Regulation of Speech on the Internet: Fourth Time's The Charm?', 11 Media Law & Policy 50, 2002, p. 60
[129] *Supra*, n. 75, p. 70
[130] *Supra*, n. 58, p. 12
[131] Council of Europe, 'Recommendation of the Committee of Ministers to Member States on Measures to Promote the Respect for Freedom of Expression and Information with Regard to Internet Filters', CM/Rec(2008)6, <https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75>
[132] *Supra*, n. 127

declares that access to Internet content can be blocked 'if the competent national authorities have taken a provisional or final decision on its illegality'.

Another concern about blocking applications is the re-emergence of blocked websites under another name. The European Union's revised Action Plan on Terrorism[133], issued in May 2006, abolished the provisions of a previous document, which obliged ISPs to block access to terrorist propaganda which they hosted. The previous provisions were regarded as inefficient because the blocked websites would usually simply re-appear under different names.[134]

Hatred content is accessible on the Internet by means of various formats such as websites, newsgroups or forums.[135] Because of this easy accessibility, racism, xenophobia and terrorism have been the main targets of the fight against hate materials at European level. The Additional Protocol to the Convention on Cybercrime[136] aims to criminalise acts of a racist and xenophobic nature committed using computer systems. Furthermore, the Council of Europe's Convention on the Prevention of Terrorism[137] criminalises acts such as 'public provocation to commit terrorist offences', 'recruitment for terrorism' and 'training for terrorism'.[138] Although it is considered vital to fight against these activities, Akdeniz and Altıparmak reveal that these regulations do not include any blocking provisions, and focus on criminalising the acts of dissemination and publication.[139]

---

[133] European Council, 'EU Plan of Action on Combating Terrorism – Update', <http://ue.eu.int/uedocs/cmsUpload/EUplan16090.pdf>

[134] European Commission, 'Commission Staff Working Document, Accompanying Document to the Proposal for a Council Framework Decision Amending Framework Decision 2002/475/JHA on Combating Terrorism', SEC(2007) 1424, Brussels, 6 November 2007

[135] A. Guinchard, 'Hate Crime in Cyberspace: The Challenges of Substantive Criminal Law', Information and Communication Technology Law, Forthcoming, 9 April 2009, p.23, <http://ssrn.com/abstract=1375589>

[136] Council of Europe, 'Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems', Strasbourg, 28 January 2003, <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>

[137] Council of Europe, 'Convention on the Prevention of Terrorism', Warsaw, 16 May 2005, <http://conventions.coe.int/Treaty/en/Treaties/Html/196.htm>

[138] *Supra*, n. 113, p. 7

[139] *Supra*, n. 75, p. 78

In summary, at European level, access blocking even for crimes such as terrorism, racism and xenophobia is not prioritized. This is due to the fact that blocking applications are acknowledged as having the potential to infringe the right to freedom of expression. Accordingly, general access blocking methods should not be permitted without taking into account the boundaries set out in the ECHR.

2.2.4 Liabilities of ISPs

An ISP is considered as to be an essential mechanism for providing access to the Internet, and for enabling the hosting of Internet content. Due to its particular features, this mechanism is utilised as a means for blocking or removing illegal and harmful content from the Internet.[140] Due to the large volume of content circulating on the Internet, Hanley does not find holding ISPs liable for monitoring of all content to be a realistic solution.[141] In contrast to systems which hold ISPs absolutely liable for illegal content, the European approach only holds ISPs liable in limited circumstances.

The EC Directive on Electronic Commerce[142] is an important regulation which reflects the European approach to the issue of ISP liability. Article 12 indicates that an ISP, as an access provider, is exempt from liability for information transmitted on condition that it is a 'mere conduit'. As to the ISP as a hosting provider, Article 14 of the Directive states that the provider will not be liable for information stored if:

> '(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity is apparent; or

[140] E. Gelbstein, J. Kurbalija, 'Internet Governance Issues, Actors and Divides', The Information Society Library: Getting the Best Out of Cyberspace & GKP Issues Paper, Knowledge for Development Series, p.71, <http://www.diplomacy.edu/ISL/IG/>
[141] *Supra*, n. 32, p. 1008
[142] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 17 July 2000, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF>

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access of the information.'

These provisions provide the basis for the Notice and Take Down (NTD) liability system, which was developed in order to deal with illegal content.[143] The NTD regime is also referred to as 'delegated self-regulation', because of the delegation of powers by Member States to ISPs.[144] According to this system, an ISP is liable for illegal content if it has actual knowledge of that content. In order not to be held liable, an ISP is required to act promptly to remove illegal content when it is notified of its presence through a self-regulatory hot-line, or by administrative agencies or the courts.[145]

Ahlert et al. argue that the concept of 'actual knowledge' is not clear.[146] For instance, if a hot-line notice is considered to constitute actual knowledge of illegal content, an ISP will be legally obliged to remove that content.[147] According to them, in ascertaining whether an Internet site contains illegal or harmful content, an ISP is required to 'assume the role of judge, jury and enforcer at the same time.'[148]

Moreover, although it is regarded as reducing the high costs of litigation; Ahlert et al. assert that NTD actually increases the burden on ISPs, by requiring them to investigate all allegations of violations.[149] Therefore, in order to avoid this burden, ISPs prefer to block access to allegedly illegal content instead of conducting investigations into complaints.[150] Frydman and Rorive state that ISPs are encouraged to remove any 'defamatory, dangerous, seditious, inaccurate or otherwise illegal or damaging content' as soon as they

[143] *Supra*, n. 75, p. 70
[144] C. Ahlert, C. Marsden, C. Yung, 'How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation', p.2, <http://www.scribd.com/doc/18560262/Liberty-Disappeared-From-Cyberspace>
[145] *Supra*, n. 55, p. 34
[146] *Supra*, n. 144, p. 10
[147] PCMLP - IAPCODE, 'Self-Regulation of Digital Media Converging on the Internet: Industry Codes of Conduct in Sectoral Analysis', 30 April 2004, p.45, <http://ec.europa.eu/information_society/activities/sip/archived/docs/pdf/projects/iapcode_executive_summary.pdf>
[148] *Supra*, n. 144, p. 27
[149] *Supra*, n. 144, p. 7-8
[150] *Supra*, n. 144, p. 12

are notified. They assert that this situation creates a 'chilling effect' on freedom of expression on the Internet.[151] They also claim that some ISPs will refrain from hosting or giving access to content that seems 'questionable, unorthodox or disturbing', in order to ensure their reputation in the marketplace.[152]

Furthermore, Frydman and Rorive criticise the NTD due to the lack of 'put back procedure' in the Directive.[153] Ahlert et al. criticise the Directive because it lacks standards for the NTD procedures.[154] They also claim that the NTD provides challenges for freedom of expression owing to a lack of transparency and accountability.[155]

In summary, the NTD liability system does indeed place an additional burden on ISPs. However, it is submitted that the NTD would be a beneficial alternative to general blocking applications in dealing with illegal content, if concerns about freedom of expression were to be eliminated. In this respect, Ahlert et al. are correct in arguing that ISPs should take down illegal content based on a decision by a court, instead of a hot-line notice. This approach would decrease the ISP's burden, since investigating claims of violations is the duty of the courts.

[151] B. Frydman, I. Rorive, 'Regulating Internet Content through Intermediaries in Europe and the USA', p.56, <http://www.isys.ucl.ac.be/etudes/cours/linf2202/Frydman_&_Rorive_2002.pdf>
[152] *Supra*, n. 151, p. 57
[153] *Supra*, n. 151, p. 51
[154] *Supra*, n. 144, p. 9
[155] *Supra*, n. 144, p. 3

3. FREEDOM OF EXPRESSION AND INTERNET CONTENT REGULATION

3.1 Freedom of Expression on the Internet

Freedom of expression is a fundamental human right which provides a basis for values such as democracy and personal independence. Thanks to the freedom of expression, individuals have an opportunity to express themselves through open debates in various fields.[156] Freedom of expression enables individuals to take part in the dissemination and creation of ideas without frontiers.[157] The Internet, as a *sui generis* medium for imparting and receiving information and ideas,[158] has become a significant ground for executing the right to freedom of expression.[159]

It is generally held that freedom of expression principles are entirely applicable to the Internet.[160] For instance, Hussain indicates that international human right standards should be applied to expression on the Internet.[161] Uyttendaele and Dumortier assert that, as freedom of expression is a media-neutral principle,[162] it should be applied to all media, including the Internet.[163] However, the right to freedom of expression on the Internet is not absolute, as are other rights. Due to the Internet being used for illegal and harmful purposes, freedom of expression on the Internet is restricted by means of Internet content regulations.

However, a government is not allowed to use the weapon of Internet content regulation arbitrarily. In fact, there is no case-law regarding freedom of

[156] *Supra*, n. 2, p. 33
[157] J. M. Balkin, 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society', 79 N.Y.U. L. Rev. 1, 2004, p.3
[158] *Supra*, n. 2, p. 36
[159] *Supra*, n. 57, p. 1
[160] *Supra*, n. 3
[161] United Nations Economic and Social Council, 'Civil and Political Rights, Including the Question of Freedom of Expression', E/CN4/2001/64,13 February 2001, p.19, <http://www.iidh.ed.cr/comunidades/libertadexpresion/docs/le_relator/e-cn%204-2001-64%20en.htm>
[162] C. Uyttendaele, J. Dumortier, 'Free Speech on the Information Superhighway: European Perspectives', 16 J. Marshall J. Computer & Info. L. 905, p.910
[163] *Supra*, n. 162, p. 914

expression on the Internet,[164] but it is understood from the ECtHR rulings that the principles which prevent governments from arbitrary interference with freedom of expression are also applicable to Internet content regulations. For instance, in *Autronic AG* v. *Switzerland,*[165] the ECtHR held that,

> the right to freedom of expression applies not only to the content of information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive information.

According to the Organisation for Economic Co-operation and Development (OECD), any restrictions on the Internet should be subject to the principles of freedom of expression.[166]

At this point, principles of freedom of expression come to the forefront in protecting individuals' rights from arbitrary interference by the government. This situation implies a negative obligation on the part of a government not to intervene arbitrarily in an individual's right to freedom of expression. Besides the negative obligation not to interfere, the government also has a positive obligation to intervene, so as to protect individuals from private restrictions.[167]

Considering self-regulation tools within the context of Internet content regulations, individuals' rights to freedom of expression are subjected to restrictions by private entities such as ISPs.[168] Jørgensen claims that on-line expression should not be restricted by private entities. He describes self-regulation as 'privatized censorship', and evaluates that ISPs constrain the grounds of freedom of expression 'by demanding a certain decency standard of their customers'. He believes that restrictions put in place by ISPs should

---

[164] P. van Dijk, F. van Hoof, A. van Rijn, L. Zwaak (eds.), *Theory and Practice of the European Convention on Human Rights*, Fourth Edition, Intersentia, 2006, p.783
[165] *Autronic AG* v. *Switzerland*, Application No. 12726/87, Series A no. 178
[166] Organisation for Economic Co-Operation and Development, 'Global Information Infrastructure-Global Information Society: Policy Requirements', Committee for Information, Computers and Communications Policy, 1997, p.65 <https://www.oecd.org/dataoecd/33/16/2095135.pdf>
[167] *Supra*, n. 2, p. 38
[168] *Supra*, n. 2, p. 34

be supervised by the government in order to guarantee that freedom of expression is protected.[169]

It is pertinent to note that this approach arises from ECtHR case-law. In *Özgür Gündem* v. *Turkey,*[170] it was held that a

> …genuine, effective exercise of this freedom does not depend merely on the State's duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals.

Having regard to both negative and positive government obligations, it is necessary to examine the enforcement of freedom of expression principles which prevent governments from arbitrarily interfering with the freedom of expression.

3.2 Article 10 of the ECHR

In this section, the principles which arise both from Article 10 of the ECHR and ECtHR case-law, and their application to the Internet content regulations, will be dealt with.

The ECHR was adopted by members of the Council of Europe in 1950.[171] The ECHR deals with the protection of various human rights, such as the right to life, the right to liberty and security, and the right to a fair trial. Article 10 - regarding the freedom of expression - has a special place among the rights in the ECHR due to its key role for the development of a democratic society.[172] The freedoms and restrictions contained in Article 10 are applicable to all mediums, including the Internet. In this respect, the compatibility of internet content regulations with freedom of expression has a significant impact on building a democratic society.

---

[169] *Supra*, n. 47, p. 62
[170] *Özgür Gündem* v. *Turkey*, Application No. 23144/93, 16 March 2000
[171] *Supra*, n. 3
[172] *Supra*, n. 164, p. 774

Article 10 is shaped in two paragraphs: the first paragraph describes the scope of the freedom, whilst the second defines the conditions required for legitimate interference with the freedom of expression.[173]

According to Article 10(1), the right to freedom of expression consists of three aspects: the freedom to hold opinions, the freedom to impart information and ideas, and the freedom to receive information and ideas. This provision also states that these freedoms must be exercised freely, without interference by public authorities and regardless of frontiers. In *Handyside* v. *the United Kingdom*, the ECtHR indicated that,

> Article 10 protects not only 'the information or ideas that are favourably received or regarded as inoffensive or as a matter of indifference, but also those that offend, shock or disturb; such are the demands of that pluralism, tolerance and broad-mindedness without which there is no democratic society.

Article 10(2) reads:

> 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.

Article 10(2), as well as ECtHR case-law, stipulates three cumulative conditions for legitimate government intervention with the freedom of

[173] M. Macovei, 'Freedom of Expression: A guide to the Implementation of Article 10 of the European Convention on Human Rights', Human Rights Handbooks, No. 2, p.7, <http://www.coe.int/T/E/Human_rights/hrhb2.pdf>

expression on the Internet.[174] In other words, governments are entitled to interfere with the exercise of freedom of expression in cases where all these conditions are met.[175] Otherwise, unjustified interference by the government would lead to a violation of freedom of expression.[176]

The first condition requires that any interference or restriction to the freedom of expression must be prescribed by law.[177] Secondly, the interference must aim to protect one or more of the following interests or values: national security, territorial integrity, public safety, prevention of disorder or crime, protection of health, morals, reputation or rights of others, preventing the disclosure of information received in confidence, and maintaining the authority and impartiality of the judiciary.[178] Thirdly, any restrictions on freedom of expression must be necessary in a democratic society. The restriction to free speech must be proportionate to its legitimate aim, and there must also be a pressing social need for the restriction in a specific situation.[179]

3.2.1 Prescribed by Law

This requirement means that any restriction to the freedom of expression must be regulated by national legislation.[180] The interference with freedom of expression can only be implemented through democratic legitimacy, which requires the use of parliamentary procedures.[181] Thus, any interference with Article 10 must be authorised by the national Parliament of the State concerned.[182] However, the ECtHR has not been satisfied solely with the presence of the law; it also asks for 'quality of law' in order to fulfil this requirement.[183]

---

[174] *Supra*, n. 162, p. 924
[175] *Supra*, n. 173, p. 29
[176] *Supra*, n. 173, p. 30
[177] *Supra*, n. 164, p. 334
[178] *Supra*, n. 173, p. 29
[179] E. Barendt, *Freedom of Speech*, Oxford University Press, 2005, p. 65
[180] *Supra*, n. 173, p. 30
[181] *Supra*, n. 173, p. 31
[182] H. Fenwick, G. Phillipson, *Media Freedom under the Human Rights Act*, Oxford, 2006, p.47
[183] *Supra*, n. 164, p. 337

In *Sunday Times* v. *The United Kingdom,*[184] in explaining the two conditions for the requirement of 'prescribed by law', the ECtHR held that:

> Firstly, the law has to be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.

In the *Rotaru* v. *Romania* case,[185] the ECtHR did not consider the national law to be law due to its unclear formulation, which did not 'enable any individual to regulate his conduct.' In *Malone* v. *The United Kingdom,*[186] the ECtHR held that the phrase 'prescribed by law' implies '… that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded'.

In *Suominen* v. *Finland,*[187] the ECtHR held that,

> …even though a domestic court has a certain margin of appreciation when choosing arguments in a particular case and admitting evidence in support of the parties' submissions, an authority is obliged to justify its activities by giving reasons for its decisions.

The ECtHR case-law requires national courts to analyse the quality of laws that restrict the exercise of freedom of expression.[188] In this respect, according to the ECtHR, there are three standards necessary in order to determine the quality of a law.

---

[184] *Sunday Times* v. *The United Kingdom*, Application No. 6538/74, Series A no. 30, 26 April 1979, para.49
[185] *Rotaru* v. *Romania*, Application No. 28341/95, 4 May 2000
[186] *Malone* v. *The United Kingdom*, Application No. 8691/79, Series A no. 82 and Series A no. 95, para.67
[187] *Suominen* v. *Finland*, Application No. 37801/97, 1 July 2003, paras. 36-37
[188] *Supra*, n. 173, p. 33

First, the law must be accessible to everyone.[189] As unpublished regulations ensure that individuals are unaware of their presence, the accessibility condition requires the law to be published.[190] Secondly, the law must be regulated precisely and clearly, so that individuals are able to understand the exact scope and meaning of that law.[191] This standard provides an important guarantee for individuals, because it enables them to 'foresee the consequences that may result from a given action'.[192] Thirdly, the law must include sufficient safeguards for individuals so as to prevent the government from applying arbitrary restrictions. The principle of the rule of law is an efficient tool for the ECtHR to provide individuals with such safeguards.[193] Having regard to the rule of law, judicial or administrative authorities must impart reasoned decisions.[194]

3.2.2 Legitimate Aims

Governments are allowed to interfere with the freedom of expression, provided that they do so on the basis of a legitimate reason as described in Article 10(2). The reasons, which are specified in Article 10(2), are exhaustive,[195] and they can be categorised into three groups. The first group aims to protect public interests, including 'national security, territorial integrity, public safety, prevention of disorder or crime, protection of health or morals'; the second group covers other individual rights, such as the protection of the reputation or rights of others, and prevention of the disclosure of information received in confidence; and finally, the last group aims to maintain the authority and impartiality of the judiciary.[196] From among these reasons, the 'protection of reputation and rights of others' and the 'protection of morals' are the most common reasons cited by governments for their interference with freedom of expression.

[189] *Supra*, n. 164, p. 337
[190] *Supra*, n. 173, p. 33
[191] *Supra*, n. 164, p. 337
[192] *Supra*, n. 162, p. 924
[193] *Supra*, n. 164, p. 337
[194] *Supra*, n. 75, p. 61
[195] *Supra*, n. 164, p. 340
[196] *Supra*, n. 33, p. 8

'Protection of reputation and rights of others' is generally used to 'protect politicians and civil servants against criticism',[197] as well as to defend the 'image/honour of the country or government', the 'image/honour of the nation' or 'State or other official symbols'. However, the ECtHR does not consider these justifications as falling within the context of a legitimate aim; this is because these justifications fall outside the scope of the legitimate aims as stated in Article 10(2). Furthermore, as everyone has a right to criticise individual officials and institutions, criticism of abstract concepts such as official symbols may not be banned by national authorities. Therefore, everyone should be free to disagree with the dominant ideology of the relevant State in order to pave the way for an efficient debate in public.[198]

Protection of historical personalities is also another issue which leads to conflict when evaluating the scope of the 'protection of reputation and rights of others'. De Baets claims that there should not be special laws for protecting historical personalities. He asserts that a right to litigate against defamation on behalf of an historical personality must be restricted. Otherwise, the law may be used as a tool to suppress different thoughts, as well as an obstacle to 'free and open debate about historical events'.[199]

As to the issue of the protection of morals, case-law indicates a wider margin of appreciation for the protection of morals in comparison with the 'protection of reputation and rights of others'.[200] In *Handyside* v. *The United Kingdom,* [201] in stating that the evaluation of morality can be different from one country to another, the ECtHR held that governments may exercise a broad margin of appreciation in assessing morality.[202] In *Müller and Others* v. *Switzerland,* [203] the ECtHR held that,

---

[197] *Supra*, n. 173, p. 49
[198] *Supra*, n. 173, p. 35
[199] A. De Baets, 'Defamation Cases against Historians', History and Theory, Vol. 41, No. 3, October 2002, p.349
[200] *Supra*, n. 2, p. 42
[201] *Handyside* v. *The United Kingdom*, Application No. 5493/72, Series A no. 24, 7 December 1976
[202] C. Ovey, R. White, *Jacobs and White: the European Convention on Human Rights*, Oxford University Press, 2006, p.332

> …by reason of their direct and continuous contact with the vital forces of their countries, State authorities are in principle in a better position than the international judge to give an opinion on the exact content of requirements of morals as well as on the "necessity" of a "restriction" or "penalty" intended to meet them.

Therefore, governments are entitled to decide whether any act infringes their particular values of morality.

These aims constitute the legal basis for restricting the exercise of the freedom of expression. However, any interference must be also necessary in a democratic society.

3.2.3 Necessary in a Democratic Society

In the *Observer and Guardian* v. *The United Kingdom* case,[204] the requirement of 'necessary in a democratic society' was evaluated as being a pressing social need for the interference, and proportional to the legitimate aim pursued.[205] These principles are the main tools for the interpretation of what constitutes a democratic necessity;[206] however, instead of considering them as alternatives, they must be taken jointly into account.[207]

3.2.3.1 Pressing Social Need Test

The 'pressing social need test' requires that the government interfere with freedom of expression in specific situations.[208] In other words, it should be a requirement that the government restrict the exercise of freedom of expression in certain circumstances.[209] In the *Handyside* case, the ECtHR

---

[203] *Müller and Others* v. *Switzerland*, Application No. 10737/84, Series A no. 133, 24 May 1988, para.35
[204] *Observer and Guardian* v. *The United Kingdom*, Application No. 13585/88, Series A no. 216, 26 November 1991
[205] *Supra*, n. 2, p. 40
[206] *Supra*, n. 164, p. 340
[207] *Supra*, n. 182, p. 94
[208] *Supra*, n. 164, p. 774
[209] *Supra*, n. 182, p. 86

referred to the margin of appreciation, which allows national authorities to assess the existence of pressing social need.[210]

However, as was stated in the *Observer and Guardian* case, the margin of appreciation 'must go hand in hand with a European supervision, embracing both the law and the decisions applying it, even those given by independent courts'. As a result of case-law, governments are allowed to determine whether there is pressing social need for any restriction to freedom of expression. However, this margin of appreciation is not absolute, and is subject to the supervision of the ECtHR.

3.2.3.2 Proportionality Test

As to the principle of proportionality, 'every formality, condition, restriction or penalty' used to restrict the freedom of expression must be proportionate to the legitimate aims stated in Article 10(2).[211] For this reason, the principle of proportionality has a widespread ground of application in the judicial systems of governments.[212] The principle of proportionality consists of tests which are used to determine whether a restriction is justified.[213] Suitability, necessity, and proportionality *sensu stricto* are the tests which are to be used in applying the principle of proportionality.[214]

In evaluating the suitability test, the main point to be focused on is the convenience of the measure for realizing the relevant legitimate aim.[215] Therefore, a causal link between the measure and the aim is vital to the

[210] J. Rivers, 'Proportionality and Variable Intensity of Review', Cambridge Law Journal, 2006, p.175
[211] *Supra*, n. 202, p. 319
[212] L. Dzabirova, 'European Proportionality in Macedonia's Political and Judicial Systems', 4 April 2009, <http://www.balkanalysis.com/2009/04/04/european-proportionality-in-macedonia%E2%80%99s-political-and-judicial-systems/>
[213] *Supra*, n. 210, p. 174
[214] J. H. Jans, 'Minimum Harmonisation and the Role of the Principle of Proportionality', p.7, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1105341>
[215] *Supra*, n. 212

suitability test.[216] The case-law of ECtHR has shown that measures taken by a government must be serve one of the legitimate aims.[217]

In the *Observer and Guardian* case, the UK applied for temporary injunctions against the Observer and Guardian newspapers, so as to prevent them from publishing 'Spycatcher', a book concerning the memoirs of a former member of the British Security Services. The UK imposed these measures within the context of protecting national security, which is a legitimate aim for a State. However, as the book was published in the US, and copies of the book were accessible outside the UK,[218] the ECtHR held that this situation stymied these measures.[219] In other words, it was indicated that the application of these measures amounted to a violation of Article 10, because the measures taken by the UK were 'no longer suitable under Article 10 after the book was published in the US'.[220]

The relationship of *Observer and Guardian* case to measures concerning Internet content is that a ban on publishing certain content is not considered suitable if the information is otherwise accessible.[221] In this respect, due to the technology and techniques which nullify the blocking measures against the undesired internet content, it is not so difficult to access prohibited content.

For instance, using a different proxy server on a non-standard port, masking Internet content before using the proxy network by changing some server names, encrypting content, and mirroring content to prevent the enforcement of the law, are some techniques which enable any individual to circumvent the law.[222] These techniques enable individuals to access information, even

---

[216] *Supra*, n. 214, p. 7
[217] *Supra*, n. 3
[218] *Supra*, n. 182, p. 98
[219] Directorate General of Human Rights, *Freedom of Expression in Europe: Case law concerning Article 10 of the European Convention of Human Rights*, Strasbourg: Council of Europe, 2007, p.13
[220] *Supra*, n. 3
[221] *Supra*, n. 3
[222] G. Hosein, 'Logical Propositions on Free Expression, Regulation, Technology, and Privacy', Panel Presentation to Global Knowledge II Action Summit, <http://personal.lse.ac.uk/hosein/pubs/gkIIprivacy.html>

where government blocking applications are in place.[223] For this reason, Lievens states that blocking tools can be circumvented easily, even by people who have limited technical skills.[224] As a result of the suitability test, it can be said that blocking applications are generally not suited to the legitimate aims.

The other aspect of the principle of proportionality is the indispensability of, and the necessity for, the measure. There are various measures which may be taken in order to interfere with Internet content, and the necessity test seeks to determine whether these measures are equally efficient in protecting the legitimate aims.[225] The other point to be focused on in relation to the necessity test is the application of the least intrusive method in order to realise a legitimate aim.[226] If the measure in question is as effective as another alternative measure, and constitutes the least restrictive measure, then it should be preferred over other possible options.[227]

Protection of morals is the issue in which governments are given the broadest margin of appreciation; that is why there are divergent instruments in order for governments to protect moral values. However, considering the user-controlled characteristics of the Internet, user-control options make government interference unnecessary in protecting morals. This is so because users such as parents or instructors are more conveniently situated than governments to control content by means of supervision, training, or filtering tools.[228] Furthermore, as an alternative method of dealing with undesirable Internet content, the NTD is a less restrictive tool in comparison with blocking applications. Therefore, in protecting moral values, government restrictions can be substituted by different methods, such as user-controls or the NTD.

The last test to be applied in relation to the principle of proportionality is the principle of proportionality *stricto sensu,*[229] or proportionality in its narrow

[223] *Supra*, n. 3
[224] *Supra*, n. 82, p. 8
[225] *Supra*, n. 214, p. 7
[226] *Supra*, n. 210, p. 198
[227] *Supra*, n. 212
[228] *Supra*, n. 3
[229] *Supra*, n. 214, p. 7

conception.[230] The main aim of this test is to strike a fair balance between the gravity of the restriction, and 'the interest in realization of the legitimate aim'.[231] The courts are required to analyse the benefits as well as the costs of the restriction. If it is realized that the cost to rights is higher than the benefits stemming from realizing the aim, then it is assumed that the restriction in question is disproportionate.[232]

Furthermore, this test requires an evaluation of whether the influences of the restriction are overly broad concerning the rights intervened.[233] According to the ECtHR, the principle of proportionality requires any restriction not to be excessive.[234] Due to the difficulties in foreseeing the most effective approach, governments may over-react to undesirable Internet content.[235] For instance, besides preventing minors from accessing harmful content, blocking measures also deprive adults of content which, for them, is legal.[236]

Moreover, the level of restrictions to be applied is also important for this test. Some blocking restrictions are applied at the level of access providers by setting a requirement for 'proxy servers'.[237] However, this kind of application paves the way for blocking access to huge amounts of legitimate content,[238] and leads to excessive and overly broad restrictions on individual rights. Besides, in the case of implementing filters at common access points, the users are obliged to be dependant on the commercial criteria of the filter. Therefore, it is suggested that filtering measures should be applied at the receiving end, instead of at the level of access providers.[239]

---

[230] K. Moller, 'Balancing and the Structure of Constitutional Rights', International Journal of Constitutional Law, 2007, p.456
[231] *Supra*, n. 182, p. 100
[232] *Supra*, n. 210, p. 200
[233] *Supra*, n. 212
[234] *Supra*, n. 3
[235] P. Samuelson, 'Five Challenges for Regulating the Global Information Society', p.6, <http://people.ischool.berkeley.edu/~pam/papers/5challenges_feb22_v2_final_.pdf>
[236] *Supra*, n. 3
[237] *Supra*, n. 30, p. 15
[238] *Supra*, n. 60, p. 8
[239] *Supra*, n. 5

4. INTERNET CONTENT REGULATIONS AND APPLICATIONS IN TURKEY

4.1 Regulatory Framework

In Turkey, the main regulations dealing with Internet content are the Law Regarding the Regulation of Publications on the Internet and Suppression of Crimes Committed via Such Publications[240] (Law No. 5651), and its secondary regulations. Law No. 5651 was enacted on 4 May 2007, and was promulgated at the Official Gazette on 22 May 2007.[241] The Regulation governing the access and hosting providers, which includes the principles and procedures for assigning activity certificates to such providers was published on 24 October 2007. In addition to the Regulation governing the mass use providers, which was published on 1 November 2007, the Regulation on the Procedures and Principles Pertaining to the Publications on the Internet[242] (Regulation) was promulgated on 30 November 2007.

The aim and the scope of Law No. 5651 is described as,

> …the determination of the undertakings and responsibilities of content providers, host providers, access providers and multiple user providers and the determination of principles and procedures for fighting against the crimes determined in the law committed on internet over content, host and access providers.[243]

The Communication Presidency (CP), a government body, is entrusted with realising these aims by means of preparing and implementing regulations.[244] The CP functions as the authority for monitoring Internet content, and

[240] TIB, 'Law Regarding the Regulation of Publications on the Internet and Suppression of Crimes Committed via Such Publications', <http://www.tib.gov.tr/node/76>
[241] Although Law No. 5651 came into force on 22 May 2007, Articles 3 and 8 only came into force on 23 November 2007.
[242] TIB, 'The Regulation on the Procedures and Principles Pertaining to the Publications on the Internet', <http://www.tib.gov.tr/node/86>
[243] Law No. 5651, Article 1
[244] Law No. 5651, Article 11

enforcing blocking orders issued by the judiciary.[245] Furthermore, the CP is charged with issuing administrative blocking orders in specific circumstances, as well as determining the minimum criteria regarding the production of hardware or software for filtering, screening and monitoring purposes.[246] Moreover, the CP is also authorised to act as a hot-line, and to report undesired content.[247] Finally, the CP is required to collaborate with related parties in terms of the assignment of blocking and filtering policies.[248]

These features of the CP demonstrate that Internet content issues in Turkey are subject to government regulation. Although the Turkish government appears to have adopted co-regulation as its method of choice for regulating Internet content, co-regulation does not work in practice due to a lack of co-operation between government and industry. In this respect, the co-regulation approach, together with a 'multi-stakeholder partnership', should be put into practice in Turkey.

Besides the CP, the providers constitute the other groups in blocking applications. In fact, in EU legislation, ISPs which provide access to the Internet also provide a unique tool for implementing Internet content regulations. However, in Turkey, the duties of the ISP are allocated to different organisations, such as Internet Access Providers (IAP), Internet Content Providers (ICP) and Host Service Providers (HSP). An ICP is any natural or legal person producing, changing and providing data offered to users on the Internet.[249] An IAP is any natural or legal person, which enables its users to access the Internet.[250] An HSP is defined as any natural or legal person providing or operating the systems that host services and contents.[251]

As to the issue of responsibility, ICPs are liable for the content they provide on their Internet sites, but they are not responsible for the content that they link

[245] Law No. 5651, Article 10(4)(c)
[246] Law No. 5651, Article 10(4)(e)
[247] Law No. 5651, Article 10(4)(d)
[248] Law No. 5651, Article 10(5)
[249] Law No. 5651, Article 2(1)(f)
[250] Law No. 5651, Article 2(1)(e)
[251] Law No. 5651, Article 2(1)(m)

to.[252] IAPs cannot be held responsible for monitoring the content that goes through their networks. Moreover, they are not required to determine whether that content is illegal or not.[253] HSPs are also not responsible for controlling the content they host.[254] However, when they are advised that they are hosting illegal content, IAPs and HSPs are required to block access to this content provided by their users, so far as it is technically possible.[255]

The 'catalogue crimes' which are regulated in Article 8 are not new crimes,[256] and are enumerated exhaustively as follows:

- Encouragement and incitement to suicide (Article 84 of the Turkish Penal Code);
- Sexual exploitation and abuse of children (Article 103(1) of the Turkish Penal Code);
- Facilitation of the use of drugs (Article 190 of the Turkish Penal Code);
- Provision of substances dangerous to health (Article 194 of the Turkish Penal Code);
- Obscenity (Article 226 of the Turkish Penal Code);
- Prostitution (Article 227 of the Turkish Penal Code);
- Gambling (Article 228 of the Turkish Penal Code);
- Crimes committed against Atatürk (Law No. 5816, dated 25 July 1951);
- Football and other sports betting websites which are based outside the Turkish jurisdiction without obtaining a valid permission.

Where adequate suspicion exists, websites on which catalogue crimes are being committed are blocked.[257] Both in preliminary investigation and at trial stage, blocking orders are granted as precautionary injunctions. In other words, these orders are not final judgments. During a preliminary investigation, blocking orders are made by a judge. In addition, the Public

[252] Law No. 5651, Article 4
[253] Law No. 5651, Article 6(2)
[254] Law No. 5651, Article 5(1)
[255] Law No. 5651, Article 6(1)(a)
[256] *Supra*, n. 75, p. 13
[257] Law No. 5651, Article 8(1)

Prosecutor can issue a blocking order where otherwise there may be a delay which is prejudicial to the investigation. However, the Public Prosecutor is required to submit the blocking order to a judge within 24 hours. If the judge does not approve the blocking order within 24 hours, the order must be rescinded by the Public Prosecutor.[258] Moreover, if a preliminary investigation does not give rise to a prosecution, the blocking order would be automatically removed.[259] At the trial stage, if the court returns an acquittal, the blocking order issued by the court would be removed.[260] Blocking orders issued by judges, courts, or Public Prosecutors are sent to the CP, which then sends these orders to IAPs to be executed.[261]

Besides the judicial authorities, the CP is authorised to issue blocking orders *ex officio*.[262] In this context, the CP functions as a hot-line which receives notices regarding undesirable content. The CP examines the technical and legal aspects of the notices which are transmitted to its hot-line. Where there is adequate evidence for suspicion, websites on which catalogue crimes are being committed will be blocked by the CP.[263] However, the CP's authority for blocking orders is subject to some conditions. The CP can issue administrative blocking orders if the content in question involves the sexual exploitation and abuse of children, or obscenity. For crimes other than the sexual exploitation and abuse of children, or obscenity, the CP can issue administrative blocking orders when the content or hosting providers are established outside the Turkish jurisdiction.[264] According to the Regulation, an order by the CP must be approved by a judge if it involves the sexual exploitation and abuse of children, or obscene content, which is hosted in Turkey.[265] If the CP locates the perpetrators responsible for the content subject to the blocking orders, the CP would request that the Chief Public Prosecutor's Office prosecute the perpetrators.[266]

[258] Law No. 5651, Article 8(2)
[259] Law No. 5651, Article 8(7)
[260] Law No. 5651, Article 8(8)
[261] Article 16(1) of the Regulation
[262] *Supra*, n. 75, p. 13
[263] Article 16(2) of the Regulation
[264] Law No. 5651, Article 8(4)
[265] Article 14(1) of the Regulation
[266] Law No. 5651, Article 8(6)

Besides the provisions regarding blocking applications, the legislation includes a *sui generis* provision, which aims to protect personal rights on the Internet. Individuals who assert that their personal rights are infringed due to content on the Internet may notify the ICP, and request it to take down the related content. If the ICP cannot be accessed, the request for taking down the related content may be conveyed to the HSP. The individuals concerned also have a right to respond to the content, and to ask the ICP or HSP to publish their responses for up to a week, on the same pages on which the contested content appeared. The ICP or HSP must abide by such request within 48 hours of receiving it.[267] Where such a request is rejected, the individual concerned may bring a lawsuit in a local Criminal Court of Peace within 15 days to ask the court to issue a take-down order, and to execute his right of response.[268]

4.2 Access Blocking Applications

Access blocking applications are examined in two different stages: the first stage consists of blocking orders issued by the courts before Law No. 5651 came into force. The second stage covers blocking orders issued by the courts and the CP since Law No. 5651 came into force.

4.2.1 Access Blocking Applications Prior to Law No. 5651

Before Law No. 5651 entered into force in May 2007, there was no specific legislation regarding Internet content blocking. In other words, a hands-off approach was adopted for regulation of Internet content.[269] In spite of the absence of specific legislation regarding Internet content regulation, the courts punished websites, such as YouTube, whose content was considered

[267] Law No. 5651, Article 9(1)
[268] Law No. 5651, Article 9(2)
[269] Privacy International and the GreenNet Educational Trust, 'Silenced: An International Report on Censorship and Control of the Internet', September 2003, p.89, <http://www.privacyinternational.org/article.shtml?cmd[347]=x-34761390&als[theme]=Silenced%20Report>

inappropriate according to the general provisions.[270] At this stage, the main reasons for granting blocking orders were terrorist activities, and insulting Atatürk and sacred values. The court orders which are referred below are only some examples of the blocking applications made before Law No. 5651 came into force.

The İstanbul 1st Criminal Court of Peace ordered blocking access to www.youtube.com due to the presence on the site of a single video including insulting expressions about Atatürk, and images defaming the Turkish Flag.[271] This video was considered illegal because insulting the memory of Atatürk is an offence under Law No. 5816, while defaming the Turkish Flag is an offence according to Article 300 of the Turkish Penal Code. Then, the Court of Peace issued a supplementary decision,[272] which stated that the blocking order would be removed if the specific content was lifted by YouTube. Thereupon, YouTube lifted the relevant video from its servers, and the access ban was brought to an end by the court.[273]

In April 2007, the İstanbul 11th Assize Court issued a blocking order for some videos on YouTube, which it considered to amount to PKK terrorist propaganda.[274] As terrorist activities are illegal under Articles 6 and 7 of the Turkish Anti-Terror Law No. 3713, the Court banned access to these pages on YouTube.

In October 2007, the Ankara 5th Criminal Court of Peace issued a blocking order in respect of some videos which it held were insulting to Atatürk, the Turkish Army, the Prime Minister and the President of Turkey.[275] This order resulted in the blocking of the whole of www.youtube.com, because of these defamatory videos.

---

[270] A. Tunç, 'Creating an Internet Culture in Turkey: Historical and Contemporary Problem Analyses', <http://soemz.euv-frankfurt-o.de/media-see/newmedia/main/articles/a_tunc.htm>
[271] İstanbul 1st Criminal Court of Peace, Decision No. 2007/384 Misc., dated 6.3.2007
[272] İstanbul 1st Criminal Court of Peace, Supplementary Decision No. 2007/384-1 Misc., dated 7.3.2007.
[273] *Supra*, n. 75, p. 27
[274] İstanbul 11th Assize Court, Decision No. 2007/842 Misc., dated 3.4.2007
[275] Ankara 5th Criminal Court of Peace, Decision No. 2007/1478 Misc., dated 24.10.2007.

4.2.2 Access Blocking Applications After the Entry into Force of Law No. 5651

Law No. 5651 now constitutes the legal basis for blocking applications in Turkey. Besides the courts, the CP also has the power to realise blocking applications. The CP started to execute court orders regarding the catalogue crimes indicated in Law No. 5651. Furthermore, court orders regarding crimes apart from those listed as catalogue crimes have also been sent to the CP for execution.[276]

As of 11 May 2009, 2,601 websites have been blocked in Turkey. 2,126 of these websites have been blocked via administrative blocking orders issued by the CP, whilst 475 have been blocked by the courts.

With regard to the 2,126 orders issued by the CP, the vast majority of these - 1,053 - involved the sexual exploitation and abuse of children, 846 involved obscenity, 117 involved gambling sites, 74 involved football and other sports betting websites, 20 involved prostitution websites, 11 involved the provision of substances dangerous to health, two involved facilitation of the use of drugs, and crimes committed against Atatürk, and one involved encouragement and incitement to suicide. As to the crimes committed against Atatürk, instead of blocking these sites, the CP has preferred to notify the ISP to take down the illegal content. The widespread application of the NTD method has led to fewer blocking orders being granted against sites accused of crimes committed against Atatürk.

In terms of the 475 court orders, 121 websites were blocked because they were deemed obscene, 54 websites were ordered to be blocked in relation to crimes committed against Atatürk, 54 websites were blocked because they involved the sexual exploitation and abuse of children, and 39 were blocked because they involved betting. In addition, five websites were blocked in relation to prostitution; three websites were blocked in relation to the

[276] *Supra*, n. 75, p. 30

encouragement of and incitement to suicide; one website was blocked because of facilitation of the use of drugs; and one website was blocked under the provision of substances dangerous to health.

197 websites were also blocked by courts for crimes falling outside the scope of Law No. 5651. It is necessary to note that the CP's blocking orders have all been issued within the scope of Law No. 5651. However, the CP has executed blocking orders issued by the courts where these did not involve the catalogue crimes listed in Article 8.[277]

The courts have issued several blocking orders both within and outside the scope of Law No. 5651. Blocking orders regarding insults to Atatürk and sacred values, obscenity, the infringement of personal rights and intellectual property rights will be dealt with next.

4.2.2.1 Insults to Atatürk and Sacred Values

After Law No. 5651 entered into force, courts began to issue successive blocking orders. In December 2007, the Ankara 11th Criminal Court of Peace held that some videos involving insulting statements about Atatürk were incompatible with Article 8(1) (b) of Law No. 5651.[278] For this reason, the Court ordered a URL-based ban, which allowed blocking access to specific YouTube pages. This court order which was the first issued under Law No. 5651 was followed by various court and administrative orders.

In January 2008, the Sivas 2nd Criminal Court of Peace,[279] the Ankara 12th Criminal Court of Peace,[280]and the İzmir 7th Criminal Court of Peace,[281] stated that YouTube must be blocked according to an IP address-based ban, because there were still videos involving defamatory statements about Atatürk on the website. The reason given for the granting of these orders was that the

[277] Güvenliweb, 'Statistics', <http://www.guvenliweb.org.tr/content/11052009-tarihli-ihbar-istatistikleri-yay%C4%B1nlanm%C4%B1%C5%9Ft%C4%B1r>
[278] Ankara 11th Criminal Court of Peace, Decision No. 2007/1431 Misc., dated 17.12.2007
[279] Sivas 2nd Criminal Court of Peace, Decision No. 2008/11 Misc., dated 16.1.2008
[280] Ankara 12th Criminal Court of Peace, Decision No. 2008/55 Misc., dated 17.1.2008
[281] Izmir 7th Criminal Court of Peace, Decision No. 2008/100 Misc., dated 29.1.2008

content was contrary to Article 8(1) (b) of Law No. 5651, and was incompatible with Article 301 of the Turkish Penal Code, which criminalises the acts of insulting Turkishness, the Republic, the organs and institutions of the State. The orders issued by these courts were significant because the scope of the catalogue crimes indicated in Article 8 of Law No. 5651 was exceeded. Although the crimes indicated in Article 301 of the Turkish Penal Code were not also included in the scope of the catalogue crimes, the courts considered Article 301 of the Turkish Penal Code as grounds for issuing blocking orders.

In March 2008, the Ankara 1st Criminal Court of Peace blocked the whole of YouTube, just as a court had done before the enactment of Law No. 5651, because of video clips containing defamatory statements made against Atatürk.[282] However, YouTube was not the only website targeted by the courts. Besides YouTube, Geocities.com, which enables users with tools to build websites, and the photo-sharing sites Slide and Tagged.com were also blocked due to the presence on their sites of defamatory statements about Atatürk.[283] The Ankara 9th Criminal Court of Peace ordered blocking access to Geocities.com in February 2008.[284] Moreover, Slide and Tagged.com were blocked by a decision of the Çivril Court of Peace.[285]

In April 2009, the Atatürkist Thought Association (ADD) put in a request to the Ankara Public Prosecutor's Office to obtain a blocking order for Google Sites. The ADD claimed that Atatürk and the concept of Turkishness were insulted in a website powered by Google Sites. Therefore, the ADD attempted to obtain a blocking order for Google Sites, because this particular website was affiliated with Google Sites.[286]

[282] Ankara 1st Criminal Court of Peace, Decision No. 2008/251 Misc., dated 12.3.2008
[283] MedyaKronik, 'Geocities de internet erişimine kapatıldı', 17 April 2008, <http://www.medyakronik.com/haber/508/>
[284] Ankara 9th Criminal Court of Peace, Decision No. 2008/140 Misc., dated 4.2.2008
[285] Çivril Criminal Court of Peace, Decision No. 2008/22, dated 24.1.2008
[286] Cyber-Rights.Org.TR, 'ADD moves to ban Google sites for defaming Atatürk in Turkey', 13 April 2009, <http://privacy.cyber-rights.org.tr/?p=390>

4.2.2.2 Obscenity

Obscenity is regulated by Article 226 of the Turkish Penal Code. The provisions of this Article are also applicable to acts committed on the Internet. As stated above, the CP has issued many administrative orders as a result of obscene content on the Internet. In November 2007, the CP issued a blocking order against a sexually explicit website hosted in Turkey, with a Turkish domain name devletim.com.tr,[287] for carrying obscene content. From November 2007 to the present date, websites such as youporn.com, redtube.com, and pornotube.com were also blocked by the CP for reasons of obscenity.

The courts have also issued numerous blocking orders because of obscene material on the Internet. For example, from November 2007 to date, websites such as fantasti.cc were banned under Article 8 of Law No. 5651.[288]

4.2.2.3 Infringement of Personal Rights

According to Article 9, individuals have right to request that content which infringes their personal rights be taken down. Furthermore, they can also force an ICP or HSP to publish their response to this content on the same website on which it was initially published. Even if such a request is rejected, the individuals in question may apply to a court to have a take-down order issued, and to execute their right to respond. Thus, the courts have issued precautionary injunctions, so as to protect personal rights, such as reputation and privacy.[289]

Adnan Oktar, who is known as a creationist author in Turkey, has benefited from the provisions of Article 9. He fights against websites which support the theory of evolution, and blogs which are defamatory to him and his beliefs. He has claimed that defamatory statements published on websites such as

[287] The order of the CP, 23.11.2007 of 2007/261190
[288] Eskişehir, 2nd Criminal Court of Peace, Decision No: 2007/1705, 23.11.2007
[289] *Supra*, n. 75, p. 37

Wordpress.com and Google Groups have infringed his personal rights. Although he requested that these websites take down these defamatory statements, they did not accede to his request. Therefore he has applied to various courts for relief, in order to protect his personal rights.

In August 2007, at Oktar's request, the Fatih 2nd Civil Court of First Instance blocked access to WordPress.com,[290] which includes over three million blogs. In March 2008, claiming that there were defamatory statements on http://groups.google.com, he obtained another blocking order, which was issued by the Silivri 2nd Civil Court of First Instance.[291] The court considered it necessary to block http://groups.google.com, so as to preclude the risk of infringement of Oktar's personal rights. However, in another case, the Gerger Civil Court of First Instance decided to remove two news articles published on www.gergerim.com and www.bianet.org which defamed the Public Prosecutor.[292] Unlike the Oktar cases, the Court did not order the blocking of websites to protect these personal rights.

4.2.2.4 Infringement of Intellectual Property Rights

In addition to Law No. 5651, Law No. 5846 on Intellectual and Artistic Works is another piece of legislation which regulates Internet access blockings.[293] Since intellectual property right infringements do not fall within the scope of Article 8 of Law No. 5651, Supplemental Article 4 of Law No. 5846 creates a specific procedure for dealing with intellectual property rights infringements on the Internet. In accordance with this procedure, after being notified by right holders of an intellectual property right infringement, HSPs, IAPs, and ICPs are required to take this content down from their servers within 72 hours. Otherwise, the right holders may request the Public Prosecutor to issue a blocking order.[294]

[290] Fatih 2nd Civil Court of First Instance, Decision No. 2007/195, dated 17.8.2007
[291] Silivri 2nd Civil Court of First Instance, Decision No: 2008/15, dated 14.3.2008
[292] Gerger Civil Court of First Instance, Decision No. 2008/1 Misc, dated 11.1.2008
[293] *Supra*, n. 75, p. 22
[294] *Supra*, n. 75, p. 37

As of January 2008, courts have used Law No. 5846 to block websites such as Justin TV due to infringements of intellectual property rights.[295] Digitürk, a digital TV platform in Turkey, holds the right to broadcast live coverage of Turkish football league matches.[296] Digitürk revealed that some blog entries on Blogger and Blogspot provided links to websites which broadcast live football league matches through its LigTV channel. Because of the pirate broadcasts made by blogs, Digitürk requested Blogger.com to take down the blog entries at issue. However, since Blogger did not respond to Digitürk's request, Digitürk petitioned the court to block access to the relevant websites. As a result, the Diyarbakır First Criminal Court of Peace banned access to the blogging services Blogger and Blogspot,[297] using supplemental Article 4 of Law No. 5846.

Furthermore, as a result of enforcing Law No. 5846, some websites providing access to pirated music and movie content are also blocked in Turkey.[298]

4.3 Assessment of Turkish Case

In this section, Internet content regulations and applications in Turkey will be assessed in light of the principles of freedom of expression.

- **Distinction between Harmful and Illegal Content in the Legislation**

Article 8 of Law No. 5651 covers the specific catalogue crimes which are regulated by various provisions contained in the relevant legislation. However, the contents which are related with these crimes are all indicated as undesirable content and they are all subject to access blocking applications. Since there is no distinction between harmful and illegal content in Turkish legislation, these crimes are subject to the same legal consequences. In other

[295] İstanbul Küçükçekmece 2nd Criminal Court of Peace, Decision No. 2008/114, dated 23.1.2008
[296] CyberLaw Blog, 'Live football streaming piracy seems to be the cause of access blocking to blogger.com in Turkey', 26 October 2008, <http://cyberlaw.org.uk/2008/10/26/live-football-streaming-piracy-seems-to-be-the-cause-of-access-blocking-to-bloggercom-in-turkey/>
[297] Diyarbakır 1st Criminal Court of Peace, Decision No. 2008/2761, dated 20.10.2008
[298] The order of the CP, 4.12.2007 of 2007/1715

words, the courts and the CP have issued a number of decisions in order to protect minors from undesirable content, but these decisions have given rise to interference with adults' freedom of expression, by means of restricting their access to legal content.[299] It is argued that this situation is not compatible with Article 10(1) of the ECHR which regulates the freedom to receive information and ideas without interference by public authorities and regardless of frontiers.

For this reason, in line with the European approach, 'undesirable' Internet content should be distinguished from 'illegal' and 'harmful' content in Turkish legislation. On one hand, crimes related to the encouragement of and incitement to suicide, the sexual exploitation and abuse of children, prostitution, facilitation of the use of drugs, provision of substances dangerous to health, and gambling or illegal betting, should be regarded as 'illegal' content. On the other hand, obscenity on the Internet should be considered to constitute 'harmful' content.

In addition to distinguishing between illegal and harmful content, regulation tools should also be distinguished according to whether they will be utilised in respect of illegal or harmful content. It is submitted that government regulations and self-regulation tools should go hand-in-hand in the fight against illegal content. However, it is argued that government regulation is not an appropriate method for dealing with harmful content, since it affects adults' right to access adult pornography. Therefore, in Turkey, the government should stand back from regulating harmful content, and should encourage users to use self-regulation tools in dealing with harmful content. However, since filtering technologies that block access to legitimate content for adults also give rise to infringements of freedom of expression, self-regulatory tools should be applied, so that adults' rights to access to adult pornography is not prohibited.

[299] Freedom House, 'Freedom on the Net: A Global Assessment of Internet and Digital Media', <http://www.freedomhouse.org/printer_friendly.cfm?page=384&key=212&parent=19&report=79>

- **Court Decisions in Respect of Content Blocking or Removal Applications**

The CP is a government body and functions as a hot-line besides its various legal responsibilities. As a result of being a hot-line, the CP is authorised to evaluate relevant Internet content in accordance with Turkish law. However, it is argued that a determination of illegality by hot-lines is inappropriate, as the authority for determining illegality should belong solely to the courts.

The CP also has the right to remove or block content. The CP can issue an administrative blocking order, if the content in question involves the sexual exploitation and abuse of children, or obscenity. For crimes other than sexual exploitation and the abuse of children, or obscenity, the CP can issue administrative blocking orders when the content or hosting providers are established outside Turkish jurisdiction. As per Law No. 5651, the CP can issue administrative blocking orders *ex officio*. However, Article 22 of the Turkish Constitution[300] states that freedom of communication can only be restricted by a court decision. It is obvious that the competence of the CP is contrary to the Turkish Constitution. Considering this conflict, in the Regulation, the CP has stated that its orders must be approved by a judge in cases of the sexual exploitation and abuse of children or obscene content hosted in Turkey. However, it is argued that all applications should be subject to judicial scrutiny.[301]

Furthermore, the power given to the CP to order to issue blocking applications is done in order to assist the judicial authorities. However, under Turkish legislation, the same power is also given to public prosecutors.[302] For this reason, it is redundant to provide such powers to the CP in addition to public prosecutors. When admitting the necessity for court decisions for blocking

[300] Turkish Constitution, <http://www.anayasa.gov.tr/images/loaded/pdf_dosyalari/THE_CONSTITUTION_OF_THE_REPUBLIC_OF_TURKEY.pdf>
[301] *Supra*, n. 75, p. 18
[302] M. V. Dülger, 'Turkey: The Evaluation of the Prevention of Internet Access and the Provisions of the Law 5651', 18 December 2008, <http://www.allbusiness.com/crime-law-enforcement-corrections/criminal-offenses-fraud/12110841-1.html>

applications, judges and prosecutors should take into account the principles of freedom of expression when deciding on Internet content-related cases. Moreover, specialist courts which are required to analyse Internet content-related cases only should be established. It is argued here that the specialist courts, charged with taking into account the inherent characteristics of the Internet, would make better and more precise decisions in relation to controversial Internet content cases.

- **The Scope of Blocking and Removal Applications**

Law No. 5651 and Law No. 5846 on Intellectual and Artistic Works are legislative tools for regulating Internet access blockings. The crimes that are included in the scope of these laws are enumerated exhaustively. This means that it is against the law to issue blocking orders for crimes apart from those listed in Law No. 5651 and Law No. 5846.

However, in practice, the courts have issued several blocking orders outside the scope of these laws. For instance, the courts have also blocked websites due to the infringement of the Anti-Terror Law and Article 301 of the Turkish Criminal Code,[303] which involves defamatory statements against 'Turkishness'.[304] As to the principle of being 'prescribed by law', the interference with the freedom of expression must have some basis in national law. However, it is submitted that blocking orders which are issued apart from Law No. 5651 and Law No. 5846 have no legal basis in Turkish law. Therefore, these blocking orders are not compatible with the principle of being 'prescribed by law'.

- **The Lack of Clarity in the Definition of Obscenity**

Some crimes which are enumerated in Article 8 suffer from definitional problems. The lack of clarity and uncertainty regarding the definitions of these crimes pave the way for controversy in terms of freedom of expression.[305]

[303] *Supra*, n. 75, p. 48
[304] *Supra*, n. 299
[305] *Supra*, n. 75, p. 47

For instance, the concept of obscenity is not defined in the text of the Turkish Penal Code. Taking into account the preamble of Article 226, indecent materials and products which disturb modesty emotions of general public are considered as obscene. However, it is pertinent to state that the criteria for obscenity are rather subjective, and can change from time to time and from person to person. Accordingly, the courts are given a wide power of discretion in determining obscenity. Since the concept of obscenity does not have any clear definition in Turkish legislation, it is observed that blocking orders for obscene content lead to arbitrary applications.[306]

According to the principle of being 'prescribed by law', the law must be delineated precisely and clearly, so that individuals are able to understand the exact scope and meaning of that law. This standard is an important guarantee for individuals, because they can 'foresee the consequences that may result from a given action'. Thus, it is considered that blocking applications associated with obscenity are incompatible with this standard, due to the lack of a clear meaning of the term 'obscenity'.

- **Absence of Reasoned Decisions**

In Turkish practice, the ICPs are not properly notified of the reasons for making the blocking decisions.[307] Websites which have been blocked are not officially informed of the reasons underlying the court decisions.[308] Since the blocking decisions are not transparent, it is very difficult to appeal against these decisions.[309]

According to the principle of being 'prescribed by law', the law must include sufficient safeguards for individuals, so as to prevent arbitrary restrictions by the State. The principle of the rule of law is an efficient tool for the court to provide individuals with such safeguards. Having regard to the rule of law,

[306] *Supra*, n. 302
[307] *Supra*, n. 75, p. 47
[308] Reporters without Borders, 'Illegal Court Ban on Websites Deplored', 8 April 2008, <http://www.rsf.org/article.php3?id_article=26484>
[309] *Supra*, n. 299

judicial or administrative authorities must impart reasoned decisions. In this respect, blocking decisions handed down without any reasoning are not made in accordance with the principle of being 'prescribed by law'.

- **NTD and Access Blocking Applications**

In Turkish practice, there are mainly two ways of interfering with Internet content: general access blocking, and the NTD applications. General access blocking is the most prevalent method used in dealing with undesirable content. On the other hand, the NTD method is applied in two different fields as per Turkish legislation.

According to Articles 5 and 6 of Law No. 5651, if the CP notifies the IAP or HSP about illegal content, they are required to take down the relevant content. For instance, as regards crimes committed against Atatürk, instead of blocking the content, the CP prefers to notify the IAP or HSP to take down the relevant content. The NTD has been successfully executed by the CP; this has demonstrated that the NTD can be used in practice rather than blocking applications.

According to the necessity test, if the measure in question is as effective as another, alternative measure, and is the least restrictive measure, then it should be preferred to other possible options. Considering the consequences of these measures, it is obvious that the NTD is less restrictive than general blocking applications. Accordingly, it can be said that general blocking applications are not necessary, and should be replaced by the NTD method.

The NTD system has some shortcomings which relate to the absence of an underlying court decision. However, it is held that the NTD system will provide a beneficial alternative to general blocking applications, if the NTD is applied in such a way so that the IAP or HSP will take down illegal content on the issuance of a court decision, instead of a CP notice.

The other area in which the NTD is applicable is Article 9 of Law No. 5651. Individuals who claim that their personal rights have been violated by content on the Internet may notify the ICP or the HSP to take down that content. These individuals also have the right to respond to that content, and to ask the ICP or HSP to publish their responses on the same pages. Should an individual's request be rejected, that individual can bring a lawsuit in a court, and ask the court to issue a take-down order, and to permit him to execute his right to respond.

According to this type of NTD system, individuals who claim that their personal rights are infringed have only the right to notify the Internet content to related parties.[310] It is understood from the wording of Article 9 that an access blocking application is not adopted within the framework of Article 9.[311] For this reason, it is argued that the courts should issue take-down orders for content infringing personal rights rather than access blocking. Otherwise, using the access blocking method for personal right infringements would fall outside of the scope of Article 9. Since the blocking method is not embraced in Article 9, using the access blocking method for personal right infringements would not be compatible with the principle of being 'prescribed by law', which indicates that 'the interference with the Convention right must have some basis in national law'.

- **Circumvention of the Law**

Blocking applications became so widespread that Turkish users began to react instantly to circumvent these applications. Methods which may be used to circumvent blocking applications are so widely available that almost every user can benefit from them. Even daily newspapers have published articles informing users about technical methods they may use to access blocked websites, such as YouTube.[312]

[310] Y. Akdeniz, K. Altıparmak, 'Adnan Hoca v. İnternet: Tüm Kapatmalar Hukuka Aykırı', p.2, <http://cyberlaw.org.uk/wp-content/uploads/2008/10/vatan-engelleme-makale.pdf>
[311] *Supra*, n. 75, p. 19
[312] *Supra*, n. 299

Using a different proxy server on a non-standard port, masking Internet content before using the proxy network by changing some server names, and mirroring content are some of the methods which enable users to circumvent the law.[313] Furthermore, websites such as 'Ktunnel.com' and 'Vtunnel.com' are used to by-pass bans on blocked websites. These websites have gained popularity by virtue of blocking applications,[314] and have started to climb into the top 50 alexa.com ranking. Moreover, according to Alexa statistics, Youtube.com is the 5th most accessed website in Turkey in spite of the blocking applications.[315]

Another discrepancy in relation to Internet restrictions regards Atatürk, who was well-known for his reformist and modernist approaches. Blocking websites which defame Atatürk is not a suitable way to protect him; this is because blocking applications not only prevent users from accessing defamatory content about Atatürk, but it also hinders users from accessing content which favours him. Moreover, considering the well-known fact that prohibitions attract great attention, it has been realised that blocked content which defames Atatürk has been highlighted by Internet users. This situation demonstrates that the protection of historical personalities on the Internet may cause unexpected consequences.

The Turkish experience reveals the fact that there is always an alternative method to access to information in spite of blocking applications. The popularity of banned websites in Turkey demonstrates that circumvention is always possible, and that blocking orders have not produced the expected results. According to the suitability test, measures performed by a government must be suitable to serve one of the legitimate aims. However, it can be said that blocking applications in Turkey are not suited to the aim pursued.

---

[313] *Supra*, n. 222
[314] Zaman, 'İşte internet yasakçılık ligi', 22 August 2007, <http://www.zaman.com.tr/haber.do?haberno=728737>
[315] Alexa, 'Top Sites in Turkey', <http://www.alexa.com/topsites/countries;0/TR>

- **Excessive Restrictions**

As to Turkish practice, two methods are used for the execution of blocking applications: DNS blocking/tampering and IP address blocking.[316] These methods are applied at the level of IAPs. The application of these methods at the level of access providers paves the way for blocking the whole content on a specific server. For instance, a legal and beneficial website such as YouTube may be blocked by virtue of a single video contained in it.[317]

However, the principle of proportionality *stricto sensu* aims to strike a fair balance between the gravity of the restriction, and 'the interest in realization of the legitimate aim'. As to this principle, the impact of the intervention should not be excessive regarding the restricted rights. In this context, blocking restrictions which are applied at the level of access providers (by DNS blocking/tampering or IP address blocking), results in blocking huge amounts of legitimate content, and leads to excessive and over-broad restrictions on individual rights.

The Turkish practice demonstrates that the cost of blocking a website is higher than the benefits stemming from realizing the aim, so it is considered that wholesale closure of a website is disproportionate. For this reason, restrictions should be applied at the receiving end, rather than applying blocking applications at the access providers' level.

[316] *Supra*, n. 75, p. 54
[317] E. Önderoğlu, 'Media Monitoring Report', 6 February 2008, <http://www.bianet.org/english/minorities/104719-bia-2007-media-monitoring-report-full-text>

5. CONCLUSION

The Internet provides unprecedented opportunities for individuals to enjoy their right to freedom of expression. However, abuse of this freedom by irresponsible users has resulted in the emergence of undesirable Internet content. This situation has obliged rule-makers to create regulative responses to deleterious content on the Internet. In this context, government regulation, self-regulation and co-regulation have taken centre stage as the main types of Internet content regulation.

As each type of regulation has its advantages and disadvantages, the identification of an efficient type of regulation is not a simple task for governments. Government regulation has advantageous aspects, such as democratic legitimacy and direct enforceability, but it also suffers from shortcomings. Self-regulation, which emerged against deficiencies of government regulation, is also afflicted with handicaps. This situation reveals the fact that self-regulation should be supported by government regulation by means of a new regulatory tool, called co-regulation. Co-regulation benefits from the enforceability of government regulation, as well as the flexibility of self-regulation. For this reason, co-regulatory solutions have been encouraged in different European regulations.

Although a tendency to shift from government regulation to self- regulation or co-regulation can be seen through various European regulations, the administration of Internet governance in Turkey is linked with government. The CP functions as the government body responsible for preparing and implementing regulations, enforcing blocking orders issued by judiciary, issuing administrative blocking orders in specific circumstances, and determining the minimum criteria regarding the production of hardware or software for filtering, and operating a hot-line. Considering the European approach, the co-regulation with a ‘multi-stakeholder partnership’ should be applied in Turkey.

Internet content regulation is a tool which is used for restricting the freedom of expression on the Internet. However, these restrictions cannot be applied arbitrarily, and they are subject to universal human rights standards. In this context, the Turkish practice of intervention in Internet content should be compatible with principles of freedom of expression established in Article 10 of the ECHR and the case-law of ECtHR. However, Turkish legislation and applications regarding Internet content have some deficiencies in conforming to the principles of freedom of expression.

For instance, absence of a distinction between harmful and illegal content in Turkish legislation has paved the way for restricting adults' access to legal content, such as adult pornography. It is argued that this kind of restriction violates Article 10(1) of the ECHR which regulates the freedom to receive information and ideas without interference by public authorities and regardless of frontiers. Therefore, obscenity on the Internet should be considered to be 'harmful' content, while other crimes listed in Article 8 should be regulated as 'illegal' content. Moreover, in cases of illegal content, government and self-regulation tools should be used together. However, in line with the European approach, the government should refrain from regulating harmful content, and should encourage users to use self-regulation tools in dealing with harmful content. Self-regulatory tools should be exploited carefully, so that the right to access legitimate content is not prohibited.

Another problematic point is the lack of clarity surrounding the definition of 'obscenity' in Turkish legislation. According to the principle of being 'prescribed by law', the definition of obscenity should be clear, so that individuals may understand the exact scope and meaning of that term. Therefore, the unclear scope of obscenity leads to arbitrary blocking orders, which are incompatible with the principle of being 'prescribed by law'.

Moreover, the CP determines the illegality of content in line with its responsibilities as a hot-line. However, the authority for determining the illegality of content should lie solely with the courts, because it is not appropriate for either the CP or any other non-governmental body to judge the

illegality of Internet content. The CP can also issue administrative blocking orders *ex officio*, but only some of these orders require a judge's approval. However, according to the Turkish Constitution, all blocking orders should be subject to judicial scrutiny.

In the meantime, Turkish practice has demonstrated that judges do not take into account the principles of freedom of expression when deciding on Internet content-related cases. Furthermore, the blocked websites are not clearly notified of the reasons for the blocking decisions being made. However, issuing blocking decisions without giving any reasons is incompatible with the principle of being 'prescribed by law'. Therefore, specialist courts which examine Internet content-related cases only, and which give reasoned decisions within the framework of freedom of expression principles should be established.

According to Turkish legislation, blocking orders can only be issued within the framework of Article 8 of Law No. 5651, and Law No. 5846 on Intellectual and Artistic Works. However, in practice, blocking orders are issued without regard for the legal scope of blocking applications. In other words, blocking orders which are issued outside the scope of Article 8 of Law No. 5651 and Law No. 5846 do not have a legal basis in Turkish law. For instance, although the blocking method is not embraced in Article 9 of Law No. 5651, the courts still block access for personal right infringements. Accordingly, these applications are not compatible with the principle of being 'prescribed by law', which requires that the interference with the freedom of expression has some basis in national law.

Besides access blocking applications, Turkish law prescribes an alternative method in dealing with undesirable content, which is called the NTD. It is generally accepted that the NTD is less restrictive than general blocking applications. The effectiveness of the NTD is demonstrated by the CP, through successful applications for crimes committed against Atatürk. Although access blocking even for crimes such as terrorism, racism and xenophobia is not prioritized at European level, in Turkish practice, access

blocking applications still constitute the more prevalent method in comparison with the NTD. As a result of the necessity test, the effectiveness and less restrictive features of the NTD should make it preferable to blocking applications. Therefore, taking into account the features of the NTD, the widespread application of general blocking applications is not compatible with the necessity test. Furthermore, the NTD should be applied with a slight variation, in that the IAP or HSP should only take down illegal content on issuance of a court decision, rather than a CP notice.

The main aim of blocking applications is to prevent users from accessing certain websites. However, Turkish experience shows that blocking applications do not serve the purpose of the law. Circumventing these applications is so simple that almost everyone can flout the bans on websites. Websites which are used for circumvention, and blocked websites, are among the most accessed websites in Turkey. This situation indicates that blocking orders have not created the expected results. Having regard to the test of suitability, which requires any measures taken to be suited to serving one of the legitimate aims, it is pertinent to say that blocking applications in Turkey are not suited to the identified aim.

Furthermore, another adverse effect of blocking applications results from the protection of Atatürk. It is true that blocking applications aim to prevent defamatory content about Atatürk on the Internet; however, banned content which defames Atatürk is accessed much more frequently than content which favours him. Moreover, blocking applications leave Atatürk unprotected, because blocking a website also paves the way for blocking all content which praises him. This situation reveals the fact that protection of historical personalities on the Internet by blocking applications may cause unexpected consequences. Therefore, as regards the suitability test, blocking applications for the purpose of protecting Atatürk are not suitable for serving legitimate aims.

In Turkey, the methods which are used for blocking applications are applied at the level of access providers. This situation gives rise to access to a legal

website being blocked because of a single video which appears on that site. On the other hand, the principle of proportionality *stricto sensu* strikes a fair balance between the restriction and the interest in realization of the legitimate aim. Contrary to this principle, application of blocking restrictions at the level of access providers brings about excessive and overbroad restrictions on individual rights. Therefore, restrictions on websites should be applied at the receiving end, instead of at access providers' level.

In conclusion, it can be said that Turkish content regulations and applications are not compatible with the principles associated with the freedom of expression. Accordingly, the relevant legislation and its application should be reviewed in the light of these principles.

BIBLIOGRAPHY

I. Books

Baldwin R., Cave M., *Understanding Regulation: Theory, Strategy, and Practice*, Oxford University Press, 1999, p. 126, 127

Barendt E., *Freedom of Speech*, Oxford University Press, 2005, p. 65

Directorate General of Human Rights, *Freedom of Expression in Europe: Case law concerning Article 10 of the European Convention of Human Rights*, Strasbourg: Council of Europe, 2007, p. 13

Fenwick H., Phillipson G., *Media Freedom under the Human Rights Act*, Oxford, 2006, p. 47 - 100

Goldsmith J., Wu T., *Who Controls the Internet? Illusions of Borderless World,* Oxford University Press, 2006, p. 142 -181

Jørgensen R. F., *Human Rights in the Global Information Society*, Cambridge, Mass.: MIT Press, 2006, p. 62, 63

Ovey C., White R., *Jacobs and White: the European Convention on Human Rights*, Oxford University Press, 2006, p. 319 – 332

Price M. E., Verhulst S. G., *Self-regulation and the Internet*, The Hague: Kluwer Law International, 2005, p. 10

Tambini D., Leonardi D., Marsden C., *Codifying Cyberspace: Communications self-regulation in the age of Internet convergence*, Routledge, 2008, p. 3 - 302

Van Dijk P., Van Hoof F., Van Rijn A., Zwaak L. (eds.), *Theory and Practice of the European Convention on Human Rights*, Fourth Edition, Intersentia, 2006, p. 334 - 783

Walden I., Angel J., *Telecommunications Law and Regulation*, OUP, 2nd Edition, 2005, p. 417

II. Articles

Ahlert C., Marsden C., Yung C., 'How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation', p. 2 - 27, <http://www.scribd.com/doc/18560262/Liberty-Disappeared-From-Cyberspace>, accessed 30 August 2009

Akdeniz Y., 'Internet Governance, and Freedom in Turkey', 2003, p. 2 - 7, <http://www.cyber-rights.org/documents/osce_turkey_paper.pdf>, accessed 30 August 2009

Akdeniz Y., 'Internet Governance: Towards the Modernization of Policy Making Process in Turkey', Papatya, October 2003, p. 2 – 29, <http://www.cyber-rights.org/documents/beyaz_kitap_english.pdf>, accessed 30 August 2009

Akdeniz Y., 'Stocktaking on Efforts to Combat Racism on the Internet', High Level Seminar on Racism and the Internet, Geneva, January 2006, p. 33 - 35, <http://www.cyber-rights.org/reports/ya_un_paper_int_06.pdf>, accessed 30 August 2009

Akdeniz Y., Altıparmak K., 'Internet: Restricted Access A Critical Assessment of Internet Content Regulation and Censorship in Turkey', November 2008, p. 13 – 78, <http://www.cyber-rights.org/reports/internet_restricted_colour.pdf>, accessed 30 August 2009

Akdeniz Y., Altıparmak K., 'Adnan Hoca v. İnternet: Tüm Kapatmalar Hukuka Aykırı', p. 2, <http://cyberlaw.org.uk/wp-content/uploads/2008/10/vatan-engelleme-makale.pdf>, accessed 30 August 2009

Akdeniz Y., 'The Regulation of Pornography and Child Pornography on the Internet', 28 February 1997, p. 32, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=41684>, accessed 30 August 2009

Article19.org, 'Background Paper on Freedom of Expression and Internet Regulation for the International Seminar on Promoting Freedom of Expression with the Three Specialised International Mandates', London, United Kingdom, 19 - 20 November 2001, p. 1 - 10, <http://www.article19.org/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf>, accessed 30 August 2009

Balkin J. M., 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society', 79 N.Y.U. L. Rev. 1, 2004, p. 3

Barlow J. P., 'A Declaration of the Independence of Cyberspace', Davos, Switzerland, 8 February 1996, <http://www.lafraze.net/nbernard/misc/Declaration-Final.html>, accessed 30 August 2009

Black J., 'Constitutionalising Self-Regulation', 59 Mod. L. Rev. 24, 1996, p. 27

Brown I., 'Internet Censorship: Be Careful What You Ask for, forthcoming', 2008, p. 8, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1026597>, accessed 30 August 2009

Cabe T., 'Regulation of Speech on the Internet: Fourth Time's The Charm?', 11 Media Law & Policy 50, 2002, p. 8 - 60

Canbay C., 'Internet Content Regulation: Comparative Analysis of Turkish and English Legislation', Dissertation, University of Essex, 2007, p. 13

Cave J., Marsden C., '*Quis custodiet ipsos custodies* in the Internet: Self-regulation as a Threat and a Promise', 28 September 2008, p. 7 - 35,

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1366723>, accessed 30 August 2009

De Baets A., 'Defamation Cases against Historians', History and Theory, Vol. 41, No. 3, October 2002, p. 349

Dunne D., 'Governance of Controversial Internet Content in the European Union', Minor Dissertation, University College Dublin, 1997, p. 4 - 54, <http://www.danieldunne.com/dunnethesis.pdf>, accessed 30 August 2009

Dülger M. V., 'Turkey: The Evaluation of the Prevention of Internet Access and the Provisions of the Law 5651', 18 December 2008, <http://www.allbusiness.com/crime-law-enforcement-corrections/criminal-offenses-fraud/12110841-1.html>, accessed 30 August 2009

Dzabirova L., 'European Proportionality in Macedonia's Political and Judicial Systems', 4 April 2009, <http://www.balkanalysis.com/2009/04/04/european-proportionality-in-macedonia%E2%80%99s-political-and-judicial-systems/>, accessed 30 August 2009

Edelstein J. I., 'Anonymity and International Law Enforcement in Cyberspace', 7 Fordham Intellectual Property, Media & Entertainment Law Journal, 1996, p. 284

Fagin M., 'Regulating Speech across Borders: Technology vs. Values', 9 Mich. Telecomm. Tech. L. Rev. 395, p. 403

Frydman B., Rorive I., 'Regulating Internet Content through Intermediaries in Europe and the USA', p. 51 - 57, <http://www.isys.ucl.ac.be/etudes/cours/linf2202/Frydman_&_Rorive_2002.pdf>, accessed 30 August 2009

Geist M., 'Cyberlaw 2.0', 44 B.C. L. Rev 323, March 2003, p. 328 - 331

Gelbstein E., Kurbalija J., 'Internet Governance Issues, Actors and Divides', The Information Society Library: Getting the Best Out of Cyberspace & GKP Issues Paper, Knowledge for Development Series, p. 71, <http://www.diplomacy.edu/ISL/IG/>, accessed 30 August 2009

Guinchard A., 'Hate Crime in Cyberspace: The Challenges of Substantive Criminal Law', Information and Communication Technology Law, Forthcoming, 9 April 2009, p. 23, <http://ssrn.com/abstract=1375589>, accessed 30 August 2009

Hanley S. M., 'International Internet Regulation: A Multinational Approach', 16 J. Marshall J. Computer & Info. L. 997, 1998, p. 1007 - 1022

Hosein G., 'Logical Propositions on Free Expression, Regulation, Technology, and Privacy', Panel Presentation to Global Knowledge II Action Summit, <http://personal.lse.ac.uk/hosein/pubs/gkIIprivacy.html>, accessed 30 August 2009

Jans J. H., 'Minimum Harmonisation and the Role of the Principle of Proportionality', p. 7, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1105341>, accessed 30 August 2009

Johnson D. R., Post D., 'Law and Borders -The Rise of Law in Cyberspace', 48 Stan. L. Rev. 1995-1996, p. 1367

Jørgensen R. F., 'Internet and Freedom of Expression', European Master Degree in Human Rights and Democratisation 2000-2001, Raoul Wallenberg Institute, 2001, p. 5 - 42, <http://www.ifla.org/files/faife/publications/ife03.pdf>, accessed 30 August 2009

Kiškis M., Petrauskas R., 'Internet Content Regulation: Implications for E-Government', The Journal of Information, Law and Technology (JILT),

2005(2), <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2005_2-3/kiskis-petrauskas/>, accessed 30 August 2009

Koomen K., 'Emerging Trends: Content Regulation in Australia and Some International Developments', AIC Conference, Sydney, 21-22 May 1997, p. 4, <http://www.acma.gov.au/webwr/aba/newspubs/speeches/documents/kkaic_97.pdf>, accessed 30 August 2009

Lievens E., 'Harmful New Media Content: The Latest Regulatory Trends', Communications Law, 2006, p. 6 - 8

Macovei M., 'Freedom of Expression: A guide to the Implementation of Article 10 of the European Convention on Human Rights' , Human Rights Handbooks, No. 2, p. 7 - 49, <http://www.coe.int/T/E/Human_rights/hrhb2.pdf>, accessed 30 August 2009

Marzouki M., '10 Years of Internet Content Regulation in Europe: Empowering or Infantilizing Citizens?', 17th International Conference on Computers, Freedom and Privacy, Montréal, Canada, 1 - 4 May 2007, <http://www-polytic.lip6.fr/article.php3?id_article=174>, accessed 30 August 2009

Marzouki M., 'Combating Racism on the Internet while Upholding International Human Rights Standards', 19 January 2006, <http://www-polytic.lip6.fr/imp-article.php3?id_article=127>, accessed 30 August 2009

Moller K., 'Balancing and the Structure of Constitutional Rights', International Journal of Constitutional Law, 2007, p. 456

Mueller M. L., 'The New Cyber-Conservatism: Goldsmith/Wu and the Premature Triumphalism of the Territorial Nation-State: A review of Goldsmith and Wu's Who Controls the Internet? Illusions of a Borderless World', p. 4, <http://internetgovernance.org/pdf/MM-goldsmithWu.pdf>, accessed 30 August 2009

Nachbar T. B., ‘Paradox and Structure: Relying on Government Regulation to Preserve the Internet's Unregulated Character’, 85 Minn. L. Rev. 215, November 2000, p. 224 - 260

Niere B., ‘European Commission: Communication on illegal and harmful content on the Internet and Green Paper on the protection of minors and human dignity’, IRIS Legal Observations of the European Audiovisual Observatory, IRIS 1996-10:4/3, p. 1

Oswell D., ‘The Dark Side of Cyberspace: Internet Content Regulation and Child Protection’, Convergence: The International Journal of Research into New Media Technologies, p. 46, 47, <http://con.sagepub.com/cgi/reprint/5/4/42>, accessed 30 August 2009

Peers S., ‘Strengthening Security and Fundamental Freedoms on the Internet - An EU Policy on the Fight against Cyber Crime’, p. 7 - 28, <http://www.europarl.europa.eu/activities/committees/studies/download.do?file=24233>, accessed 30 August 2009

Rivers J., ‘Proportionality and Variable Intensity of Review’, Cambridge Law Journal, 2006, p. 174 – 200

Samuelson P., ‘Five Challenges for Regulating the Global Information Society’, p. 6, <http://people.ischool.berkeley.edu/~pam/papers/5challenges_feb22_v2_final_.pdf>, accessed 30 August 2009

Schönberger V. M., ‘The Shape of Governance: Analyzing the World of Internet Regulation’, Virginia Journal of International Law, Spring 2003, p. 612

Schultz T., ‘Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface’, The European Journal of International Law, Vol. 19 no.4, EJIL, 2008, p. 839

Tunç A., ‘Creating an Internet Culture in Turkey: Historical and Contemporary Problem Analyses’, <http://soemz.euv-frankfurt-o.de/media-see/newmedia/main/articles/a_tunc.htm>, accessed 30 August 2009

Uyttendaele C., Dumortier J., ‘Free Speech on the Information Superhighway: European Perspectives’, 16 J. Marshall J. Computer & Info. L. 905, p. 910 - 924

Valcke P., Stevens D., Lievens E., Werkers E., ‘Audiovisual Media Services in the EU Next Generation Approach or Old Wine in New Barrels?’, p. 107 - 109, <http://www.law.kuleuven.be/icri/publications/1149CS71_VALCKE_et_al.pdf?where=>, accessed 30 August 2009

Walker CP, Akdeniz Y., ‘The Governance of the Internet in Europe with Special Reference to Illegal and Harmful Content’, Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet, 1998, p. 5 -12

Walker C., ‘Cyber-Contempt: Fair Trials and the Internet’, Yearbook of Media and Entertainment Law 1997, p. 537

Weinberg J., 'Rating the Net', Hastings Communication and Entertainment Law Journal 453, 1997, <http://faculty.law.wayne.edu/Weinberg/rating.htm>, accessed 30 August 2009

Westfall J., ‘Internet Blocking’, Santa Clara University, <http://www.scu.edu/ethics/publications/submitted/westfall/blocking.html>, accessed 30 August 2009

III. Reports

Bertelsmann Foundation, ‘Self-regulation of Internet Content’, Gütersloh, 1999, p. 15 - 45, <http://www.cdt.org/speech/BertelsmannProposal.pdf>, accessed 30 August 2009

Capitanchik D., Whine M., 'The Governance of Cyberspace: Racism on the Internet', JPR/Policy Paper, No. 2, 1996, <http://www.jpr.org.uk/Reports/CS_Reports/PP_2_1996/index.htm>, accessed 30 August 2009

EICN, 'Report on Internet Governance', July 2005, p. 3 - 6, <http://www.clubofamsterdam.com/contentarticles/28%20Governance/Report%20on%20Internet%20Governance.pdf>, accessed 30 August 2009

First Report of Working Group, 'Illegal and Harmful Use of the Internet', p. 2, <http://ec.europa.eu/avpolicy/docs/reg/minors/useinternet1streport_ie.pdf>, accessed 30 August 2009

Global Internet Liberty Campaign, 'Regardless of Frontiers: Protecting the Human Right to Freedom of Expression on the Global Internet', <http://gilc.org/speech/report/>, accessed 30 August 2009

ICC, 'The Impact of Internet Content Regulation', Commission on E-Business, IT and Telecoms, 18 November 2002, <http://iccwbo.org/id510/index.html>, accessed 30 August 2009

INHOPE, 'The International Association of Internet Hotlines, Towards Online Safety: Taking Action Today, Ready for Tomorrow', Third Report, 2006, p. 8, <https://www.inhope.org/system/files/inhope_report_2006.pdf>, accessed 30 August 2009

Marsden C., Simmons S., Brown I., Woods L., Peake A., Robinson N., Hoorens S., Klautzer L., 'Options for and Effectiveness of Internet Self- and Co-Regulation Phase 2: Case Study Report', 15 January 2008, <http://ssrn.com/abstract=1281374>, accessed 30 August 2009

Ofcom, 'Identifying Appropriate Regulatory Solutions: Principles for Analysing Self- and Co-Regulation', 10 December 2008, p. 8 - 24,

<http://www.ofcom.org.uk/consult/condocs/coregulation/statement/statement.pdf>, accessed 30 August 2009

Organisation for Economic Co-Operation and Development, 'Global Information Infrastructure-Global Information Society: Policy Requirements', Committee for Information, Computers and Communications Policy, 1997, p. 65, <https://www.oecd.org/dataoecd/33/16/2095135.pdf>, accessed 30 August 2009

Önderoğlu E., 'Media Monitoring Report', 6 February 2008, <http://www.bianet.org/english/minorities/104719-bia-2007-media-monitoring-report-full-text>, accessed 30 August 2009

PCMLP - IAPCODE, 'Self-Regulation of Digital Media Converging on the Internet: Industry Codes of Conduct in Sectoral Analysis', 30 April 2004, p. 45, <http://ec.europa.eu/information_society/activities/sip/archived/docs/pdf/projects/iapcode_executive_summary.pdf>, accessed 30 August 2009

Privacy International and the GreenNet Educational Trust, 'Silenced: An International Report on Censorship and Control of the Internet', September 2003, p. 89, <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347 61390&als[theme]=Silenced%20Report>, accessed 30 August 2009

IV. Turkish Court Decisions and CP Orders

Ankara 5th Criminal Court of Peace, Decision No. 2007/1478 Misc., dated 24.10.2007

Ankara 11th Criminal Court of Peace, Decision No. 2007/1431 Misc., dated 17.12.2007

Ankara 12th Criminal Court of Peace, Decision No. 2008/55 Misc., dated 17.1.2008

Ankara 1st Criminal Court of Peace, Decision No. 2008/251 Misc., dated 12.3.2008

Ankara 9th Criminal Court of Peace, Decision No. 2008/140 Misc., dated 4.2.2008
Çivril Criminal Court of Peace, Decision No. 2008/22, dated 24.1.2008
Diyarbakır 1st Criminal Court of Peace, Decision No. 2008/2761, dated 20.10.2008
Eskişehir, 2nd Criminal Court of Peace, Decision No: 2007/1705, dated 23.11.2007
Fatih 2nd Civil Court of First Instance, Decision No. 2007/195, dated 17.8.2007
Gerger Civil Court of First Instance, Decision No. 2008/1 Misc, dated 11.1.2008
İstanbul 1st Criminal Court of Peace, Decision No. 2007/384 Misc., dated 6.3.2007
İstanbul 1st Criminal Court of Peace, Supplementary Decision No. 2007/384-1 Misc., dated 7.3.2007
İstanbul 11th Assize Court, Decision No. 2007/842 Misc., dated 3.4.2007
İstanbul Küçükçekmece 2nd Criminal Court of Peace, Decision No. 2008/114, dated 23.1.2008
İzmir 7th Criminal Court of Peace, Decision No. 2008/100 Misc., dated 29.1.2008
Silivri 2nd Civil Court of First Instance, Decision No: 2008/15, dated 14.3.2008
Sivas 2nd Criminal Court of Peace, Decision No. 2008/11 Misc., dated 16.1.2008
The order of the CP, 23.11.2007 of 2007/261190
The order of the CP, 04.12.2007 of 2007/1715

V. ECtHR Decisions

Autronic AG v. *Switzerland*, Application No. 12726/87, Series A no. 178
Handyside v. *The United Kingdom*, Application No. 5493/72, Series A no. 24, 7 December 1976
Malone v. *The United Kingdom*, Application No. 8691/79, Series A no. 82 and Series A no. 95

Müller and Others v. *Switzerland*, Application No. 10737/84, Series A no. 133, 24 May 1988
Observer and Guardian v. *The United Kingdom*, Application No. 13585/88, Series A no. 216, 26 November 1991
Özgür Gündem v. *Turkey*, Application No. 23144/93, 16 March 2000
Rotaru v. *Romania*, Application No. 28341/95, 4 May 2000
Sunday Times v. *The United Kingdom*, Application No. 6538/74, Series A no. 30, 26 April 1979
Suominen v. *Finland*, Application No. 37801/97, 1 July 2003

VI. International Documents and Legislation

Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 Amending Council Directive 89/552/EEC on the Coordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States Concerning the Pursuit of Television Broadcasting Activities, 18 December 2007

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 17 July 2000, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF>, accessed 30 August 2009

European Parliament and Council of the European Union, 'Recommendation on the Protection of Minors and Human Dignity and on the Right of Reply in Relation to the Competitiveness of the European Audiovisual and On-line Information Services Industry', (2006/952/EC), 20 December 2006, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:378:0072:0077:EN:PDF>, accessed 30 August 2009

European Commission, 'Communication on Illegal and Harmful Content on the Internet', COM(96) 487 final, Brussels, 16 October 1996, <http://aei.pitt.edu/5895/01/001527_1.pdf>, accessed 30 August 2009

European Commission, 'European Union Approach to Illegal and Harmful Content on the Internet', <http://www.copacommission.org/meetings/hearing3/eu.test.pdf>, accessed 30 August 2009

European Parliament and Council of the European Union, 'Decision on Adopting a Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks', No. 276/1999/EC, OJ L 33, 25 January 1999

The Council of the European Union, 'Council Framework Decision of on Combating the Sexual Exploitation of Children and Child Pornography', 10748/03, Brussels, 29 July 2003, <http://register.consilium.eu.int/pdf/en/03/st10/st10748en03.pdf>, accessed 30 August 2009

Council of Europe, 'Declaration on Freedom of Communication on the Internet', 28 May 2003, <https://wcd.coe.int/ViewDoc.jsp?id=37031>, accessed 30 August 2009

Council of Europe, 'Recommendation of the Committee of Ministers to Member States on Measures to Promote the Respect for Freedom of Expression and Information with Regard to Internet Filters', CM/Rec(2008)6, <https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75>, accessed 30 August 2009

European Council, 'EU Plan of Action on Combating Terrorism – Update', <http://ue.eu.int/uedocs/cmsUpload/EUplan16090.pdf>, accessed 30 August 2009

European Commission, 'Commission Staff Working Document, Accompanying Document to the Proposal for a Council Framework Decision Amending Framework Decision 2002/475/JHA on Combating Terrorism', SEC(2007) 1424, Brussels, 6 November 2007

European Commission, 'Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services', COM(96) 483, Brussels, 16 October1996,<http://aei.pitt.edu/1163/01/minors_info_soc_gp_COM_96_483.pdf>, accessed 30 August 2009

European Commission, 'Communication from the Commission to the Council and the European Parliament, Better Regulation for Growth and Jobs in the European Union', Com(2005) 97 Final, Brussels, 16 March 2005, <http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0097en01.pdf>, accessed 30 August 2009

Council of Europe, 'Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems', Strasbourg, 28 January 2003, <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>, accessed 30 August 2009

Council of Europe, 'Convention on the Prevention of Terrorism', Warsaw, 16 May 2005, <http://conventions.coe.int/Treaty/en/Treaties/Html/196.htm>, accessed 30 August 2009

United Nations Economic and Social Council, 'Civil and Political Rights, Including the Question of Freedom of Expression', E/CN.4/2001/64, 13 February 2001, p. 19, <http://www.iidh.ed.cr/comunidades/libertadexpresion/docs/le_relator/e-cn%204-2001-64%20en.htm>, accessed 30 August 2009

VII. Turkish Law

Turkish Constitution, <http://www.anayasa.gov.tr/images/loaded/pdf_dosyalari/THE_CONSTITUTION_OF_THE_REPUBLIC_OF_TURKEY.pdf>, accessed 30 August 2009

TIB, 'Law Regarding the Regulation of Publications on the Internet and Suppression of Crimes Committed via Such Publications', <http://www.tib.gov.tr/node/76>, accessed 30 August 2009

TIB, 'The Regulation on the Procedures and Principles pertaining to the Publications on the Internet', <http://www.tib.gov.tr/node/86>, accessed 30 August 2009

VIII. Others

Alexa, 'Top Sites in Turkey', <http://www.alexa.com/topsites/countries;0/TR>, accessed 30 August 2009

CyberLaw Blog, 'Live football streaming piracy seems to be the cause of access blocking to blogger.com in Turkey', 26 October 2008, <http://cyberlaw.org.uk/2008/10/26/live-football-streaming-piracy-seems-to-be-the-cause-of-access-blocking-to-bloggercom-in-turkey/>, accessed 30 August 2009

Cyber-Rights.Org.TR, 'ADD moves to ban Google sites for defaming Atatürk in Turkey', 13 April 2009, <http://privacy.cyber-rights.org.tr/?p=390>, accessed 30 August 2009

EDRI-gram, 'The French Constitutional Council censures the 3 strikes law', Number 7.12, 17 June 2009, <http://www.edri.org/book/export/html/1967>, accessed 30 August 2009

Freedom House, ‘Freedom on the Net: A Global Assessment of Internet and Digital Media’, <http://www.freedomhouse.org/printer_friendly.cfm?page=384&key=212&parent=19&report=79>, accessed 30 August 2009

Güvenliweb, ‘Statistics’, <http://www.guvenliweb.org.tr/content/11052009-tarihli-ihbar-istatistikleri-yay%C4%B1nlanm%C4%B1%C5%9Ft%C4%B1r>, accessed 30 August 2009

MedyaKronik, ‘Geocities de internet erişimine kapatıldı’, 17 April 2008, <http://www.medyakronik.com/haber/508/>, accessed 30 August 2009

Reporters without Borders, ‘Illegal Court Ban on Websites Deplored’, 8 April 2008, <http://www.rsf.org/article.php3?id_article=26484>, accessed 30 August 2009

The Internet Watch Foundation, ‘IWF Facilitation of the Blocking Initiative’, <http://www.iwf.org.uk/public/page.148.437.htm>, accessed 30 August 2009

Zaman, ‘İşte internet yasakçılık ligi’, 22 August 2007, <http://www.zaman.com.tr/haber.do?haberno=728737>, accessed 30 August 2009