T.C.
KADİR HAS UNIVERSITY
INSTITUTE OF SOCIAL SCIENCES
M.A PROGRAM IN COMMUNICATION STUDIES

SOCIAL NETWORK SITES, USER RIGHTS AND INTERNET GOVERNMENTALITY

M.A THESIS

EMİNE ECE SAÇAR

İstanbul, 2010

T.C.
KADİR HAS UNIVERSITY
INSTITUTE OF SOCIAL SCIENCES
M.A PROGRAM IN COMMUNICATION STUDIES

SOCIAL NETWORK SITES, USER RIGHTS AND INTERNET GOVERNMENTALITY

M.A THESIS

EMİNE ECE SAÇAR

Advisor
Assistant Professor LEMİ BARUH
Associate Professor LEVENT SOYSAL

İstanbul, 2010

ABSTRACT

SOCIAL NETWORK SITES, USER RIGHTS AND INTERNET GOVERNMENTALITY

Emine Ece Saçar

M.A Program in Communication Studies

Advisor: Lemi Baruh

December, 2010

Recently, popularity of online social network sites (SNS) has grown significantly throughout the world. On the one hand, SNS provide users with an arguably unprecedented capability to share information with others. On the other hand, globalized nature of SNS participation (and internet use in general) brings about several important issues regarding usage rights and governmentality. This thesis will focus on two issues in particular. First, users are generally unaware of the legal problems they may face when they share information and opinions via SNS. For example, increasingly, companies troll SNS sites to check for opinions that user's voice about them (including but not limited to products). Opinions that may jeopardize companies' reputations increasingly result in lawsuits targeting the users who wrote about the company. Second, and related to the first dimension, is the cross-national inconsistencies in legislations addressing online user rights create an environment that is very difficult to navigate for both online users and social network service providers.

The thesis will begin by summarizing research on social network site usage and users' motivation in using social network sites. Then, the thesis will discuss two dimensions of governmentality: "User Awareness" (Chapter 3) and in "Legislative Inconsistencies in Internet Governance" (Chapter 4). Finally, Chapter 5 will focus on three issues regarding free speech and defamation online, privacy rights of users' work place efficiency to illustrate the discussions made in the previous chapters.

Keywords: Social networks sites, online user's rights, inconsistencies in internet governance.

ÖZET

Emine Ece Saçar

İletişim Bilimleri Yüksek Lisans Programı

Danışman: Lemi Baruh

Aralık, 2010

Son yıllarda sosyal ağ sitelerinin popülaritesi ciddi oranda artmaya başlamıştır. Fakat bu sosyal ağların kullanımı bir taraftan kullanıcılara eşsiz bir bilgi paylaşım ortamı sunarken, diğer taraftan da sosyal ağ kullanımının (genel olarak internet kullanımının) global olmasından kaynaklanan sorunlara neden olmaktadır.

Bu tez iki konuya odaklanacaktır. Birincisi, kullanıcılar sosyal ağları kullanıp, burada fikirlerini açıklarken, paylaştıkları bilgi ve fikirlerin onları yasal sorunlarla karşı karşıya getirebileceğinin farkında olmamaları, ikincisi ise –birinci konuyla bağlantılı olarak- uluslararası bir ortam olan sosyal ağlarda yaşanan sorunların çözülmesinde, yasal yönden ülkeler arasında farklı ceza yöntemleri bulunması yüzünden kullanıcılar ve servis sağlayıcılarının yaşadıkları zorluklardır.

Bu konular üzerinde durulurken; sosyal ağ çeşitleri ve kullanım alanları, kullanıcıların sosyal ağ kullanım motivasyonları anlatılacak, daha sonra kullanıcının farkındalığı ve internet yönetimindeki yasal tutarsızlıklar örneklerle anlatılacaktır.

Bu çalışmanın esas amacı, sonsuz özgürlük ortamı olarak görülen internetin yaratabileceği sorunlara dikkat çekmek ve yasal açıdan ortada olan tutarsızlıklar hakkında kullanıcıyı bilgi sahibi yapmaktır.

Anahtar Kelimeler: Sosyal ağ siteleri, çevrimiçi kullanıcı hakları, internet yönetimindeki hukuksal tutarsızlıklar.

ACKNOWLEDGEMENTS

I would like to show my gratitude to Assistant Professor *Lemi Baruh* for his greatest support and help from the beginning till the end. I would like to mention his patience during my hard times, his encouragement and precious advices during the research. His support was invaluable for me.

I would also like to thank to Associate Professor *Levent Soysal and* Assistant Professor *Melis Behlil* who had been a great support during my M.A. years. I will always remember their advices and support.

I would like to show my appreciation to my mother Kezban Saçar, my father Zafer Saçar and my sister Sedef Saçar for being with me in every step that I have taken in my life with great understanding and support. They are the very reason of my success.

Contents

Contents

1. Introduction

21st century brings a new context for technology of thinking and communicating through modern tools and devices. Information flows faster than it ever has. New languages and mental maps are created independent of any geographical concerns.

Especially, social network sites have gained importance in recent years. They have millions of users and their sizes are growing day by day. There are a lot of public social network sites, such as Facebook, Twitter, YouTube, MySpace and Flickr and so on. People create online profiles and share their personal information with others via these sites. Social Network Sites affect their users both positively and negatively. For example, people can communicate more freely with others via social network sites and express themselves. But on the other hand, users generally think that there are no limits to what can say online. Many users actually believe that because they use nicknames to communicate relatively anonymously via the Internet, they can be freer in terms of voicing their opinion online. Most users are not aware of the potential legal implications of online speech/presence.

For example, in recent days, social networking sites have begun to affect users' rights (both as consumers and as employers) because the information they share via sites like Twitter can hurt the reputation of companies they write about. Users frequently share the information about the companies they work for, the products they use and the brands they have purchased. However, increasingly, companies seeking to protect their reputation will pursue these individuals via number of methods including cease and decease orders to service providers and lawsuits targeting the individuals for damages to company reputation. Part of the problem here lies at users' lack of awareness of policies governing usage rights online. What further exacerbates the issue becomes the presence of multiple jurisdictions trying to govern a global network such as the Internet. The result becomes inconsistencies regarding what users can or cannot do online. These inconsistencies influence not only how service providers like Twitter, YouTube or MySpace function in different jurisdictions but also makes it very difficult for individuals to determine what they are and are not allowed to do.

This thesis will focus on these two issues of 'user awareness' of policies and 'cross-national inconsistencies' in internet policy-making.

The second chapter will provide a brief overview of social network sites online. This chapter will summarize different types, uses and structures of social network sites. The chapter will also discuss users' characteristics and motivations in using SNS.

The third chapter will focus on users' awareness of legal implications of their online actions.

Chapter 4 will provide a detailed analysis of different national legal systems that seek to govern the Internet. Information crimes are brand new issues in countries' agendas. There is a definition of how the information crimes emerged. And social networking behaviors vary from culture to culture, but it has to be same rights and same sanctions in everywhere. A monolithic development models for SNSs is likely to succeed in all over the world because our subject is World Wide Web. However, countries make changes in their legal system differently. Some of them are arranging the existing laws, but others are making new laws about information crimes. And some international organizations are making studies about this type of crimes for years; there will be a summary of these organizations.

The fourth chapter will compare and contrast similarities and differences between USA, United Kingdom and Turkey's legal system about online crimes. USA and United Kingdom are chosen because these countries are making special arrangements against online crimes and Turkey is trying to make new laws like USA and UK.

Chapter 5 will provide a detailed case study of three issues to illustrate how different jurisdictions deal with online governance. The issues that will be covered will be "free speech vs. defamation, privacy, and work place efficiency."

2. The Definition of Social Network Site

Social Network Sites as web-based services that allow individuals to:

1. Construct a public or semi-public profile within a bounded system,
2. Articulate a list of other users with whom they share a connection,
3. View and traverse their list of connections and those made by others within the system (Boyd and Ellison, 2007: 212).

On the Internet, there are different kinds of social network sites. They support different practices and interests. People who use these SNSs present themselves freely. However, because of the privacy structures of these sites, they can be accused of whatever they say. This chapter is contributing "what kind of social network sites are and what their privacy settings are" to my thesis. If all of these social networks are same, it is easy to find a solution for protecting both user and company rights. But they are not same.

For example, Facebook is one of these social network sites. Profiles in Facebook are unique pages. People can type oneself into being via this site. Facebook takes a different access-by default if a profile owner has decided to deny permission to those in their network, users who are one part of the same network can view each other's profiles. Moreover friends, comments and private messaging, SNSs vary greatly in their features and user base. Facebook groups are very proper places for self-expression and identity creation.

LinkedIn is another example of SNSs. LinkedIn is a business-oriented social networking site. Its motto is “brings together your professional network,” with the use of the tagline that “relationships matter.” LinkedIn users usually affiliate with their work network. They use the site to maintain a list of contact details for people that they know and trust within their line of work, which is termed “connections.” This network of contacts is employed to maintain communication, trade information and refer each other. The site employs a gated-access approach, meaning that connecting with others requires either a pre-existing relationship or the intervention of a mutual contact, which is a mechanism designed to facilitate trust among members(Papacharissi, 2009: 7).

Twitter is one of the most important web-site for presenting yourself. The site is constructed on the question of “What is happening” and users have only 140 characters for writing this. Users are followers of each other. In a profile page, we see the numbers of followers and followings. If users want to hide their tweets, they can do this with the privacy settings. When you hide your tweets, nobody can read your tweets without your followers. Other users must send you a request for following you, and then they can see your tweets. But if you don’t choose to protect your tweets, anyone can follow you. You do not have to follow a person who follows you.

MySpace is a SNS which is based on sharing music tastes and making new friends; YouTube is another SNS, based on videos. There are many other social networking sites, too.

2.1 Presenting oneself in SNSs

"Social networking has the potential to create an intelligent order in the current chaos by letting you manage how public you make yourself and why and who can contact you" said Tribe.net CEO Mark Pincus in an interview. Social networking sites allow people to go beyond the traditional way of presenting their identity. People can communicate with others via SNSs more easily. Moreover, according to Evans, Gosling, and Carroll (2008), what individuals have to say about themselves in social media does not fall on deaf ears: a person who views the online profile of another person usually forms impressions that are congruent with the profile owners (cited in Baruh and Soysal, 2008: 2).

People always try to present themselves in a positive manner, but this is not easy in face-to-face communication. In face-to-face communication, people cannot control their impressions on people. They have not enough time, while we are comparing online communication, for thinking and acting. People just do and bear the consequences. On the other hand, online impressions are controllable. They are often doubtful. "Online users can organize the information flow and enhance self-image by

strategically selecting how and what to convey to the receiver" (Herring and Martinson, 2004; Walther, 2007; Walther, Slovacek, and Tidwell, 2001). "Inflating or even manipulating others' perceptions of oneself has come to be expected, and no small portion of online users' disclosures involves a modicum of exaggeration, even with good chances of meeting offline observers of their online" (Ellison, Heino, and Gibbs, 2006: 11).

According to Miah, as unlike in face-to-face interaction, the Internet offers a space in which individuals can express certain strategically crafted identities. The Internet offers a valuable context in which to explore identity construction for two reasons. First, because the Internet appears to offer a seemingly limitless array of freedom of expression individuals often feel liberated. This liberation challenges identity construction and offers individuals a chance to change, modify, or challenge the identities they claim to hold (Miah, 2000: 211).

SNSs affection on people became important with the wide use of SNS. Companies started too interested in what users' sharing; they established new departments for tracking what people talk about their company online. Social network sites are getting heavy traffic on the Internet. When we search something, we see the social network sites on the top of the search. This is because they incur danger both users and companies. It can lead to bad reputation or you can be arrested. When people write a keyword on Google or a tracking program, for example: the keyword is a

company's name; they are able to see what is written about on the internet. In recent years, people start to make online searches about what they want to know, they just write about anything to know and are getting some results. Especially, they read other users opinions about what they search. After they read other others opinions, they make a decision. At this point, privacy issues have gaining importance; next chapter is giving information about user awareness and privacy issues on SNSs.

3. User Awareness and Privacy Issues

In all of these sites, people are creating their profile, and then they begin to share. *Sharing* is the basic function of these sites. When users begin to use a SNS, they share information about themselves, their environment, and their work. Also, social networking sites aim *connecting*. Connecting can be with acquaintances or strangers. When these two functions, *sharing* and *connecting* come together, they can lead to some problems. The contents that you share can be destructive for someone else or a company and a person or company which is in your network can use this information against you. They can sue you.

Social networking sites are playing an increasingly vital role in everyday social interactions. The particular role of SNSs varies across relationships—in some contexts SNSs supplement existing real-world social networks but in other contexts, interactions can be entirely mediated by SNSs (Walther and Parks, 2002: 537). When people share information about their experiences and everyday lives, they have the right to exercise information about themselves. The popular media frequently covers such distempers.

SNSs are growing in worldwide and they are very popular. Because of this popularity, SNSs have evoked many corporations to invest time and money in

creating, purchasing, promoting, and advertising on SNSs. But there is a contradiction, in terms of giving importance to SNSs usage. While some companies are making these investments, other companies are blocking their employees from accessing these sites.

Forming and managing impressions is a fundamental process for companies and one that has been complicated by new communication technologies. "As computer-mediated communication (CMC) has diffused, successive technological variations raise new questions about interpersonal impressions. For example, with people meeting via text-based CMC—e-mail, discussion groups, or chat spaces of various kinds—a variety of questions arose about impression formation and management" (Walther, Van Der Heide, Kim, Westerman and Tom Tong, 2008: 28).

These include "whether and at what rate impressions are formed online" (Walther, 1993: 28), "how online impressions may be like or unlike offline impressions" (Jacobson, 1999: 2), and "how people judge the authenticity of self-presentation online"(Donath, 1999: 29).

But with further developments of Internet-based technologies, people start to collect information about other people in other ways than direct online give-and-take. With the help of this technology, individuals are *Googleable* now and many information collecting programs are building up. The relative value of various kinds of online

information may depend on the extent that any item appears to be involuntarily associated with the person to whom it refers (Walther and Parks, 2002: 540).

SNSs are also challenging legal conceptions of privacy. Hodge (2006) argued that the fourth amendment to the U.S. Constitution and legal decisions concerning privacy are not equipped to address social network sites. For example, do police officers have the right to access content posted to Facebook without a warrant? The legality of this hinges on users expectation of privacy and whether or not Facebook profiles are considered public or private (Boyd and Ellison, 2007: 15).

Social network sites provide a lot of information about their users. The type of information can give rise to different conditions. These include: semi-public information such as current and previous schools and employers (as in Friendster); private information such as drinking and drug habits and sexual preferences and orientation (as in Nerve Personals); and open-ended entries (as in LiveJournal) (Gross and Acquisti, 2005: 2).

Because of this, user's privacy is very important. Personal information privacy is "the ability of the individual to personally control information about oneself" (Stone, Gardner, Gueutal and McClure, 1983: 459). Information technology developments are leading to a rising tide of concern about personal information privacy

management practices. As such concerns continue to grow, businesses' ability to use personal information may be threatened, and decision makers will have to make trade-offs between the efficient, effective operation of businesses and the protection of personal information privacy (Smith, 1994). The confluence of private and public is especially pronounced on a medium such as the internet, and is particularly relevant to interaction developing in online social networks (e.g. Barnes, 2006: 2; Boyd and Heer, 2006: 60; Donath and Boyd, 2004: 73). In parallel with their huge and growing acceptance among a wide range of users, social networks are becoming a focus of attention for researchers and practitioners (especially in marketing function). Also, governments and law enforcement re-awaken to the need to analyze the SNSs of terrorists and other criminals.

There are some examples of how these organizations are reacting against to social network sites usage in these places: For example, the U.S. military soldiers are banned from accessing MySpace, Canadian government suppressed employees from Facebook, while the U.S. Congress has proposed legislation to ban youth from accessing SNSs in schools and libraries (H.R, 2006: 5319). There are some other examples, such as "Kansas University decided to penalize students after finding out that the photographs they uploaded on Facebook contained evidence that they violated an alcohol policy of the University" (Acquisti and Gross, 2006: 7). Similarly, Microsoft officials frequently look over job candidates Facebook profiles.

Additionally, personal privacy issues are the most spoken topic about online world because user profiles are very important for getting personal information. People share their location, gender, age, physical attributes, race, religion, smoking and drinking habits, self-description, etc. At this point, Turkle (1999) says, it is not strange that the internet has been defined as an important social laboratory in which to explore the construction and the reconstruction of the ego, which characterizes postmodernism.

The relation between privacy and a person's social network is multi-faceted. According to Weintraub (1997), scholars invoking the public/private dichotomy typically use one of two analytically distinct metaphors. The first is what is hidden or withdrawn versus what is open, revealed, or accessible. Private things are things that we are able and/or entitled to keep hidden, sheltered, or withdrawn from others. The second line of analysis used to distinguish between the public and private concerns what is individual, or pertains only to an individual, versus what is collective, or affects the interests of a collectivity. Strahilevitz has offered applying formal social network theory as a tool for aiding interpretation of privacy in legal cases. He suggests basing conclusions regarding privacy on what the parties should have expected to follow the initial disclosure of information by someone other than the defendant.

Internet is so wide and information has flow rapidly on the internet. Corporations start to build or to buy profile-based "find-an-expert" applications like one component of their knowledge management systems because the threatening information can flow without their permission; they need to catch this information within in the shortest possible time.

Even though electronic profile applications are becoming more common, there is little known about how different ways of presenting information in profiles might affect the profile assessment process. Electronic media are characterized by their ability to remove, or at least rearrange, the boundaries between public and private spaces, affecting our lives not so much through content, but rather "by changing the 'situational geography' of social life" (Meyrowitz, 1986: 6).

According to Smith (1994), corporate policy making regarding information privacy has been primarily reactive in nature, in that executives focus on information privacy issues only in response to a perceived external threat. "An important problem concerning the vast amount of information that institutions collect about individuals is to interpret the ensuing data" (Baruh and Soysal, 2008: 6). Just as with the collection phase, a process known as *data mining* increasingly allows the use of algorithms for automatic detection of patterns that can be used to predict future behavior and risk (Gandy, 2002; Zarsky, 2002, 2004).

People leak their opinions every time, everywhere. What they say is important if there is evidence. On the Internet, people left footprints and these footprints can collect, they turn evidences and can be important only that means anything for a company. Companies have some rights and they use them against their worker. Also government or schools can apply the sanctions. When you write something about someone, somewhere or something, people or organizations can use your data on the Internet against you. However, users and workers have some rights, too. Not only organizations or companies have right to make sanctions. I will describe what kind of rights they have, the law about information crimes in next chapters.

4. Legal Inconsistency

4.1 Cross-border Governance

The Internet is not owned by a particular organization or person. The owner of the Internet is all Internet users. There is no center to technically manage the internet access of worldwide users. There are two major advantages of this decentralized governance of the Internet. First, the Internet's functioning is not dependent on the budget of a single entity. Second, the institutions do not have to make radical changes in their network structure in order to connect to the internet. Nevertheless, still some functions are managed centrally. For example, standardization of the protocols used to determine the IP addresses on the internet allows functioning of the internet in the interests of all users. Government Systems Inc. (GSI) and Internet Activities Board (IAB) are the two important management organizations. GSI is addressing IP addresses and related services; the IAB is coordinating the standardization of Internet protocols.

The disadvantage of the lack of central Internet governance is that there is no central authority enforcing sanctions against unlawful behavior on the Internet (Sınar, 2001: 30). There are two ways to prevent the Internet from being a totally unlegislated area. First one is countries started to regulate the legal responsibilities of the Internet users. Second one is the creation of rules by the Internet users which are called

"netiquette". Netiquette system is the general moral rules to be followed on the Internet (Dülger, 2004: 54). As a result, there is a wide space of freedom on the Internet. That's why the concept of the internet is perceived by some as a means to promote democracy and criticized by others due to creating confusion and chaos (Değirmenci and Yenidünya, 2003: 42).

4.1.1 Information Systems and Cultures

Westin (1967) found that every society values privacy in some form but the expressions of this privacy varies significantly across cultures. He also showed that all modern societies provide for solitude, intimacy, anonymity, and reserve. These are the four basic states of privacy. Additionally, Westin noted that variations in privacy social balances, under which privacy's states are traded off against other societal values, are noticeable even in societies that are rather homogeneous in many other reverences. These variations in privacy patterns in interpersonal relations have been observed across countries by anthropologists, psychologists, and sociologists.

Regulations and policies regarding the use of personal information differ from one country to another. Therefore, in a global marketplace dependent on trans-border data flows, understanding the differences in information privacy concerns and regulatory approaches, and the relationships between them may be a key to

successfully managing those concerns (Milberg, Burke, Smith and Kallman, 1995: Vol. 38, No. 12).

Some states prefer freedom over security, while others are limiting fundamental rights and going a number of regulations. The biggest difference that separates internet technology from other technologies is that this technology does not recognize the boundary and the structure of time. Therefore, it's not that simple to come up with regulations and this issue can only be solved by international alliances and treaties.

4.2 Information Crimes: A General Summary

There is no universally accepted definition of the information crimes. With the developing forms of technology, there is a quick change in the process of the information crimes. Because of that, defining the information crimes has become even more difficult. There is no unity in the classification of crimes because the information crimes are a new section in the legal system. The most widely accepted definition of the information crimes were described in the European Economic Community of Experts meeting in Paris on May 1983. According to this definition, "It is every type of immoral, illegal and improper action that is materialized in a system that automatically processes data or transports information." (Özel, 2002: 2, 3). As a result, today there is a commonly accepted definition of information crimes.

4.3 The History of Information Crimes

Internet is a very effective tool. Freedom and security is so intertwined on the Internet. With the heavy use of computers, information crimes have emerged. And with the emergence of the Internet, information crimes have increased and the need of the modification of the legal system appeared. The technology is developing day by day and making human life easier. A new form of living has been materialized with the technology. However, at the same time new types of crimes are emerging. Criminals have also started to use this technology. Today, the concept of the computer revolution is not only to facilitate our lives. Its name is also cited together with the concept of crime. Criminals use this technology as a tool of committing crime.

Every innovation brings new fields to the legal system, but at the same time these innovations create new rooms to violate the legal system. In recent years, information crimes have come to the attention of users and experts because Internet is a new channel and it has some flaws. When they discovered these flaws, they can employ them to their advantage. Because of this, there is a wide range of the information crimes. However, in our country information crimes are not considered as a serious crime such as murder, terrorism, etc. But, when we think about the damages of information crimes, they are in fact so serious. Legislators made

arrangements in our country in order to protect public from the people who commits cyber-crimes. These arrangements -based on new technology- made in the last 20 years.

Finally, information crimes have been put in a detailed way in the Turkish Penal Code *(Türk Ceza Kanunu)* No. 5237 and were passed in the parliament on 26.09.2004. Technically, it is not expected to be effective in practice in terms of reducing cyber-crimes at this point. We have to accept the supremacy of law in the fight against information crimes. So, the best solution is changing the legal basis in accordance with the developing conditions of day.

4.4 Types of Information Crimes

4.4.1 General Definition of Information Crimes

The most important feature that separates the information crimes from the classic types of crimes is that there is a significant difference in the patterns of processing these crimes because the information crimes have new forms of processing and types other than the classic types of crimes. On the classic types of crimes, material elements occurs physical movement, but on the information crimes there are no much physical movement, although the damage will be more than classic types of crimes.

Information crimes happen in a very short period of time and leave very few clues. They can lead to very big losses. And also the perpetrators of these crimes are more difficult to detect. Due to the rapid progress in computing technology, the ways these crimes are prosecuted has been amplified in the last few years. Information crimes are serious crimes. They have a great potential of danger to the world. Up to now, none of these crimes could have been that influential. The Internet has no borders and actions can be performed anywhere in the world. Because of the difficulty of tracking people on the Internet, this gives rise to be escaped from the hands of the law. The problem can be solved, but there is a need of international cooperation.

Especially the Council of Europe, the United Nations, European Union, the World Trade Organization, the G8 countries and international organizations like the OECD are working on the cybercrimes.

4.4.1.1 Activities of G8 Countries

The G8 is a union which consists of eight countries which has the world's most advanced industry. The studies by G8 related with information crimes have gained speed after 1995 and various study groups have been formed.

In 1995, a meeting held in Canada. The leaders have decided to build *Lyon Group* known as the Senior Experts Group on Organized Crime. Lyon Group held a meeting in France in 1995 and they published a report named *Tips on Effective Combating of International Organized Crimes*. In 1997, within the G7 (Russia is not yet member), *The High Tech Crime Sub-Committee* was formed. In addition, in order to simplify the process of investigation and prosecution, a communications group has been established which serves 24 hours. Internal affairs and foreign affairs ministers of the G8 gathered in 1997 in Washington DC, and they discussed *High Tech Crimes* and agreed upon *The 10 Principles and Actions on 10 Points Plan*. This is the final report of the conference:

i. Satisfying the protection of privacy and individual freedom,
ii. Protecting the objectives of governments in combatting against the advanced technology crimes,
iii. Including the appropriate tools to facilitate the work,
iv. Identifying transparent and exact definitions of the information crimes,
v. Ensuring free and fair activities, supporting the effectiveness of code of conduct and standards which are voluntarily determined by the private sector.
vi. Evaluating the efficacy and outcomes (http://www.gilc.org).

4.4.1.3. OECD (The Organization for Economic Co-operation and Development)

In particular, the Organization for Economic Co-operation and Development (OECD) and the Council of Europe have produced guidelines for policy makers and legislators. In 1983, OECD undertook a study of the possibility of an international application and harmonization of criminal laws to address the problem of computer crime or abuse.

OECD was expanded considerably by adding other types of abuses that were recommended as deserving of the application of the criminal law. The Select Committee of Experts on Computer-Related Crime of the Committee on Crime Problems examining these questions also addresses other areas, such as privacy protection, victims, prevention, procedural issues such as the international search and seizure of data banks, and international cooperation in the investigation and prosecution of computer crime.

In 1992, OECD developed a set of guidelines for the security of information systems, which is intended to provide a foundation on which States and the private sector may construct a framework for the security of information systems. In that same year, the Council of Europe began a study that will concentrate on procedural and international cooperation issues related to computer crime and information technology (http://www.oecd.org).

4.4.1.4 UN (United Nations)

Within the United Nations, held in 1985, first study on cyber-crimes is *Congress on Crime Prevention and Rehabilitation of Offenders,* then prepared *from the Action Plan of Milan Plan* against the crimes defined in the international action plan described in the report, between 42-44 paragraphs. Again, after the 8th congress on *Crime Prevention and Rehabilitation of Offenders*, the action plan from the effects of technological development has published. After the action plans from the effects of technological development is addressed and attention is drawn to information technology crimes. In this plan, they draw attention to the information crimes. United Nations, especially the fight against organized crime, has addressed for information solutions (http://www.uncjin.org/Documents/irpc4344.pdf).

4.4.1.5 European Council

The first serious study by the Council of Europe in 1985, a committee of experts has established for conducting of information technology crimes. The Council, with reference to the OECD report in 1986 specified here under the criminal sanction violations before the receipt of the member countries have adopted, and also included a set of principles and violations of the OECD report has not mentioned.

The OECD report also mentioned a number of principles and violations and also gave the location. In addition to the actions specified in the report of the Committee of the OECD, as a result of studies on crime prevention is connected by computer, frustration of the victims, a number of style rules, for example, the international researches, data banks and computer crime investigation and prosecution of the confiscation of a draft international cooperation in issues presented go (http://www.oecd.org).

After these studies, *European Convention on Cyber Crime* and *Committed through Information Systems for Making Racist and Criminalization of acts of foreign enemy of Europe Convention on Cybercrime Additional Protocol* were produced by the European Council.

4.4.1.6 European Union

Information crimes have entered the European Union's agenda in 1996. The meeting has organized at the same year; the main topics of the meeting were about issues of human trafficking, child sexual abuse and child protection (Sınar, 2004: 72). These organizations studies against the information crimes are still continuing. They are trying to make international cooperation.

4.5 Information Crimes in Comparative Law

Technological developments are free from boundaries. It is inevitable to make cooperation with other countries to struggle against information crimes. The Internet is an international network, because of that many difficulties are arising against the fight of crime and criminals. On the other hand, it has a very important place for this type of national regulations and restructuring in the fight against these crimes. Almost all countries made some arrangements about information crimes in their legal system.

Information technologies have entered all areas of our everyday lives. There is a noticeable improvement on information crimes, and countries started to make legal arrangements. When we explore the countries legal systems which are making some arrangements on their legal system, we see two different types. First one is to make a separate, an independent law for information crimes. And the second one is that the crimes committed in this area that there is no difference from other crimes and the arrangements had been made available only way to express the laws of digital media.

4.6.1 The Countries: Making Special Arrangements

The laws of information crimes in a distinct arrangement are seen in countries like the United States and Great Britain (Önder, 1994: 505). Some countries find this method applicable and they make special laws for information crimes and they guaranteed it.

4.6.1.1 U.S.A

The U.S.A is the fastest progressing country with the technological developments of computers and network systems. It is an example to other countries. United States has a federal structure. Almost every state has regulations regarding information crimes. Information crimes take wide place in state law than federal law. But there is no harmony between these arrangements. In fact, there are serious differences. Because of the regulations on information crimes, non-governmental organizations started the action, in the United States. Some arrangements have been cancelled by the Federal courts (Çeken, 2005: 5).

One of the important laws in the United States at the federal level is the American Foundation Act 18 of 1984, 1030. section made by replacement paragraph Computer Fraud and Abuse Act (Brenner, 2005: 25). This law was amended four times in 1988, 1989, 1990 and 1994. By this law, acts of piracy against the public agencies and

private organizations on their computers, web sites were asked to prevent from the unauthorized access. And access to a protected computer, the destruction and modification of the computer data was transformed into the crime. In general, electronic mail, voice mail, and remote control systems via the communication dated 12.10.1986 with the aim of protecting *Electronic Communication Privacy Statement Law* (the Electronic Communications Privacy Act) were carried out in the United States (Çeken, 2005: 20).

Internet Gambling Prohibition Act Law was issued on 23.07.1997, with the law about some games which is playing in the United States, which is accessible via the Internet, is banned, except in certain areas and people who make this action have been sanctioned (Mahmutoğlu, 2001: 43).

In the U.S., federal regulations, as well as qualified, has been made in various legal regulations in the provinces in order to solve the legal problems are posed by the Internet. In addition, many organizations are struggling with the crimes in the U.S. computing and there are special units of these institutions. Some of them are as follows; FBI National Infrastructure Protection Center, Information Technology Association of America, with Trap and Trace Center Authority and Emergency Response Team at Carnegie Mellon and some units are established at some universities, they are the most important part of these units. However, many public institutions have formed some units to combat this type of crime. For example, the

CIA has established a staff unit, named *Information Warfare Center* and it has 1000 guests and that generated a 24-hour service. FBI has formed a group for prosecuting crimes committed through computers in order to prosecute at the federal level, which is named *National Infrastructure Protection Center*, and *Computer Crime Squad*. These groups are organized in throughout the country. In addition, Ministry of Conservation has formed a separate section the Department of Criminal Justice, in order to protect Computer Crimes and Intellectual Property Rights, the section's name is *Computer Crime and Intellectual Property Section*. In this section, expert prosecutors are following the information crimes. In addition, a prosecutor, within each region prosecutor's office, is appointed to carry out the crimes of the information in the execution. This is the most important problem faced by the authorities while performing their duties, the complex structure of these crimes and lack of expert staff in this regard (Çeken, 2005: 30). As seen, the United States in the field of legislation and the necessary arrangements already entered the crime was carried out the necessary measures.

4.6.1.2 United Kingdom

In UK, computing crimes has been taken under the arrangement with *The Computer Misuse Act.* It is entered into force on 29.08.1990. This law consists of three chapters and 18 sections. The purpose of this law is to prevent making changes and entering computers without permission (Yazıcıoğlu, 1997: 169). The changes in *The Obscene Publication Law* and *Telecommunications Law* that have firstly been put into practice

in 1964 and 1984 respectively have brought along arrangements in pornography and child pornography. One of the most important laws in the UK is *Regulation of Investigatory Powers Act 2000* about for the rest of the Internet. The new technologies and the Internet have been added to content of the wiretapping law (Dülger, 2004: 86).

4.6.1.3 Turkey

With the emerging of computing technologies, the number of crimes which is committed in the virtual environment has increased in our country. New types of crime are organized in the *Information Crimes Chapter* and that is stated as a whole and protected regardless of the legal value in the Turkish Penal Code No.5237, dated 26.09.2004 and entered into force on 01.06.2005 Turkish Penal Code No.5237, described the crimes can be handled by anyone. The unlawful actions of the perpetrators are punished. There is no criminal liability for legal persons (Özgenç and Şahin, 2001: 131). Accordingly, legal persons, whom provide benefit from the unlawfully entering the computer system, will not be accepted as agent for the reason of 20th Penal Code No.5237, because of the perpetrator of the crime, but they will be applied with security measures in the same article but no: 60 (Kurt, 2005: 270-271).

The new Turkish Penal Code has accepted on 04.05.2007. There is a special law about *The Regulations of Internet Publications and The Struggle of the Crimes which*

is committed by these publications. The crime of insult in virtual worlds can be done with voice, video, or written. For example, a message is containing insults such as *thief, lame,* and *dishonest*, this article shall apply. This web site is a publication of the messages in the case; the penalty will be increased with the same article because the processing of the law of libel is considered qualified as a form of this crime (Özgenç, 2005: 855).

Additionally, the concepts of crime time and place are related with prosecution. They need to dwell upon on this subject. The movement is considered as the crime while it is done. In addition, crime is considered to be where they had been made. But in the crimes of the distance, result with moving parts or where a crime has been committed shall be carried out (Değirmenci and Yenidünya, 2003: 48).

4.6.2 The Countries: Making Changes in Applicable Laws

Those who choose this procedure by making changes in legislation for a number of existing provisions under regulation crimes receive the information. But in this system, there are two different opinions. The first is the legal value of the information is protected by editing the protection of the crimes. In this method, information crimes should be put in order as a whole. This type of arrangement as an example of the method determines the countries France, Luxembourg, Portugal can be (Dülger, 2004: 86). The other method is the protection of the legal value while

editing the information crimes legislation. “The concept is increasingly becoming prevalent in today's doctrine of criminal law that is that the meaning and purpose of criminal law is the protection of legal values” (Ünver, 2001: 51).

5. Cases

In recent years, courts started to teem with information cases. At the beginning use of the Internet, these cases were about mostly hackers, information stealing etc. but now they are about SNSs. Do SNSs ensure freedom of speech or is it legal liability? Which one is true? What are the privacy rights of users?

At this point, there are some cases explained above:

5.1 Free Speech vs. Defamation

Who would think that the message you share with your friends in an area less than 140 characters, will cost you 50 thousand dollars? We should be careful, while we are commenting on social networking sites. You think that you are just complaining about the grievance of any subject, this message is counted as an insult against an installed compensation can lead to stay, but how?

Amanda Bonnen is a 25 years old woman who lives in Chicago. She is being sued for defamation by a realty company that claims her tweet destructively affected the company's reputation. Horizon Group Management LLC filed a lawsuit in July against Amanda Bonnen. She allegedly took to her Twitter account to specify about

mold in her apartment building. Bonnen has told another user: "Who said sleeping in a moldy apartment was bad for you? Horizon realty thinks it's okay."

Horizon accused Bonnen of damaging their reputation, but Cook County Circuit Court Judge Diane Larsen did not think so. The case was filed in Cook County court specifically claiming that the tweeter "maliciously and wrongfully published the false and defamatory tweet on Twitter, thereby allowing the tweet to be distributed throughout the world" (http://www.blogs.findlaw.com).

The realty company owns over 1500 apartments. Bonnen had 20 followers. The tweet in question was an @ tweet, means directed to a specific user, broadcast on Amanda Bonnen's profile. And those are the facts. The intriguing legal query is whether these facts amount to evidence of defamation. In the digital age of instantaneous messaging, communication, and online sharing, how will tort claims of defamation hold up in court?

In their court filings, Bonnen's attorneys argued that her tweets were random and hyperbolic and were not statements of fact. Citing other Illinois court cases, they said a statement's literary and social context matters in determining whether it is to be taken as factual content, and therefore constitutionally protected. They noted that as a medium Twitter contains academic, casual, insightful, and silly speech that is sometimes *drivel*. Bonnen only speculates what Horizon thinks in the tweet giving

her personal opinion and not stating a fact. The tweet also doesn't give Bonnen's location or indicate she lives in property managed by Horizon to give factual background to her tweet, they argued. And the court agreed and threw the case out holding "the tweet non-actionable as a matter of law" (Huffington Post Online).

Amanda's account was closed because of her twitter message. However, on the Internet, we need to know if two people knew something, this is not a secret. Some states provided legal sanctions for false and defamatory comments. It's a discussing issue that Amanda's comment is enough to slander Horizon. But it is a fact that it reaches more people than a real complaint about the Horizon. Perhaps this event would only create social turmoil in the media. But it turns a company's reputation protection case.

Now, when we write any comments about us on sites, like Twitter, are we are we so afraid of opening cases about us? At this point, the boundaries between freedom of expression to insult or attack the brand is very difficult to draw. However, this situation can be seen as a factor for pushing to give better service to consumers.

The case is in USA. According to USA laws, Amanda Bonnen has accused of destruction of the reputation. But, the court is decided to her innocence. Her case is an example for people on same situation. Defamation laws in the United States are significantly less limiting of speech than the laws of other countries because the US

First Amendment provides strong protection for freedom of speech. If this case happens in UK, it comes to a conclusion in same way. And with the new Turkish Penal Code, Turkey take its place on countries that make special laws about information crimes.

5.2 Privacy and Work Place Efficiency

There are also some other type of cases. Privacy issues are very important in online communication as I mentioned before. For example: The chairman of the Dallas Mavericks team, Mark Cuban, he awarded damages 25.000 dollars, because of his tweets that is about the arbitrator of the Maverick-Nuggets match is not honest. Then, one of the players of NFL is punished by the team, because he made comments about meals at camp. Colin Kazım, a footballer who plays in Fenerbahçe, is also apologized from another football team, Beşiktaş. Because he insulted to Beşiktaş on Twitter, then he apologized also on the site. These players are accused of privacy sharing. They are not allowed to share their personal ideas publicly because of their contract's privacy.

Privacy cases are another part of this kind of cases on courts. Companies started to put forward reasons about workers' social networking usage for discharging. Due to the stress of working life, workers found a web site for spare their time on the

internet. These web sites are mostly SNSs. These sites have different visions –as I mentioned before- and a great source of information for some sectors, however, they contain many features that cause wasted time. Many employers prohibit such sites.

The reasons for banning these sites are the risks of falling performance and information security breaks. When you look at such sites -as the content of the information, you can find much information about people in the workplace; competitors can also collect the data about what the employees are doing at that moment. While workers share the expression of many of the psychological situation, even if the data can be obtained about the projects in these work places. On these types of sites, workers' personal information, like business locations and positions, are written clearly. This information is not a mystery in daily life. However, because of the nature and importance of the work, this kind of information can required to be hidden. The company can be an open target for their opponents. They can access know how and trade secrets. This is only a state but not limited to working hours, especially during working hours, such information-sharing and instant messaging environments are more likely to share work-related issues are also high. For this reason, the risks may arise because of these provisions by the employer indicating the beginning or just social networks, the Internet may be prohibited or restricted use.

There are two cases about workers who share the information about their work on Twitter. These cases are from Turkey. First case is experienced in an advertising

agency, in Pure New Media. One of the digital agency workers shared her difficulties about work on her blog. Then her boss was realizing what she was written. Actually, she does not give any brief information about which company or who is she. But it is not hard to find or imagine who write it. They know her blog's address and after the boss saw this entry, he fired his worker, because of this blog entry.

In another case, another worker was written about her personal situation on Twitter, but it was not relevant with work. But the boss read this tweet and she took it into her work. The second one is luckier, because she got only a warning e-mail about what she wrote. But the first one is fired.

There is no equity about these cases, because there is a lack of information about online information cases in Turkey. Some employers have been frequently referenced the term of the employment contract because of social networking and internet use. However, the termination of employment contract is not in a simple manner like "S/he was surfing on social networking sites in office hours, then we fired him/ her, it is held in favor of workers. If we take this issue in two ways, first we must deal with the matters of the employer and the employee, in the contract explicitly restricted the use of internet for personal purposes, or the presence of a similar provision". Termination of employment contract is possible in two ways. The first is, in the 18 article of the Labor Law, "the reasons were arising from worker's performance and capability" and second one is the reasons for the termination of the

current, justify the reasons for termination listed in Business Law Article 25th right to immediately terminate.

The employer may have a constituent for restricting use of social networks and the internet on the employment contract. Such a substance put through the use of the internet for breach of contract by the employee, if there is a negative point of the concrete work, based on the defense of employers and workers are expected to continue to work with or the contract may be terminated. In this case, worker's simple web getaway; it will be a case in excess of the measure to the termination of the contract for employer. In determining these criteria, the workplace and the working status of the employer are very important in terms of negativity caused by the severity of the action.

With the use of the Internet, the Supreme Court's decision is striking: Explicitly or implicitly as a special purpose without the consent of the employer, Internet is prohibited in the workplace. In other words, the employment contract, implied or otherwise expressly permitted on the worker, may use the Internet as a private Internet use at work as a special purpose. However, exceptions can be allowed in emergency situations and legitimate business reasons for the rupture.

The employer is authorized to determine the rules and instructions of the workplace. Although, it is not specified in the contract provisions of the employer, the

prohibition of personal use at work is indisputable. As a result, the use or prohibition or restriction of the Internet and personal social networks are the employer's discretion. It is a failure to comply with these instructions, despite warning no reason for termination indemnities.

In their daily lives or working places, people need to be careful what they say. There is no boundless freedom of speech on the Internet. According to these cases, we see the conclusions of unconscious use of Twitter.

6. Conclusion

The biggest difference that separates internet technology from other technologies is the timeless and boundless structure of it. Therefore, information crimes are not simple; states cannot be overcome with the regulations of legal systems. However, this can be solved by international alliances and treaties. Of course, it is not only obstructed the use of fundamental rights for security reasons. There is another aspect of this situation: People and business. Some people want to inure to the benefit of the technology to find vulnerabilities as well as employees who want to use the technology their malicious aims. These people can track and save our personal data and also want to take trade secrets. They can commercialize our profiles and our attitudes online platforms.

In all over the world and in our country, some specific internet crimes are defined in their legal systems. Laws, as well as an assurance to protect fundamental rights, sometimes they were also a good tool because of the internet and internet technologies, practitioners who do not know the limitation of fundamental rights. For this reason, the legal measures for the protection of fundamental rights are far from being effective enough. In fact, people who want to protect private data and private lives, and what personal data, personal data; the classification is who determines how much access to a “Draft Law on Personal Data Protection”, the Assembly pass into law since 1982, awaits. As a result, individuals that use Internet technology to enjoy

the benefits of this technology are not alone and someone is watching them and registering them.

People, who think about injustice, or not getting the service fully, they begin to complain on the Internet. However, there is a breach of privacy and intimacy in the virtual world growing day by day. According to the law to enter someone else's private living area and recording their information is a crime. But if the people in this situation give consent, it will create justification and not consent to penalty.

What does Twitter say? Cases of this type of site usage agreement, is entitled to delete the account, but obviously not specify a mandatory obligation, Twitter is not responsible for damages arising from communication between people. Thus, the importance of never read but always marked by the box comes to mind. “I read the agreement, I agree".

It’s a fact that compensation cases because of comments on sites like Twitter will be increased. However, who can stop social media? Maybe people should start to censor themselves. Of course, the people at the companies have the right to make comments freely in social networking sites. This damaged the reputation of the legal interest of commercial companies and the subsequent material is protected by the TCK 57. To comment about the interpretation contains an element of a crime, criminal responsibility according to the principle of privacy are also present. There is no

doubt the freedom of speech, they are protected by the Constitution, but it is not unlimited.

Bibliography

Akbulut, Berrin. 1999. *Türk Ceza Hukukunda Bilişim Suçları,* Konya: Unpublished Ph.D. Distertation.

Akçam, Bahadır K. 1999. *Suçla Mücadele Edenler İçin İnternet,* Ankara: Türk Bilişim Derneği Yayınları.

Akıncı, Hatice, A. Emre Alıç and Cüneyd Er. 2004. *Türk Ceza Kanunu ve Bilişim Suçları,* İstanbul: Bilgi Üniversitesi Yayınları.

Atasay, Rahşan. "Bilgisayar Suçları", December 12 2010. <www.turkhukuksitesi.com>.

Bailenson, Jeremy, Andrew Beall and Jack Loomis. 2004. "Transformed social interaction: Decoupling representation from behavior and form in collaborative virtual environments". November 2 2010, <http://www.stanford.edu/~bailenso/papers/TSI.pdf >.

Bailenson, Jeremy, Kim Swinth and Crystal Hoyt. 2005. "The independent and interactive effects of embodied agent appearance and behavior on self-report, cognitive, and behavioral markers of copresence in immersive virtual environments". *Teleoperators and Virtual Environments*. October 28 2010 <http://www.mitpressjournals.org/doi/abs/10.1162/1054746057747852 35?journalCode=pres >.

Barlow, John Perry. 1996. "A declaration of the independence of cyberspace". October 2010. <http://www.eff.org/~barlow/Declaration-Final.html >.

Baruh, Lemi and Levent Soysal, . 2008. *Public Intimacy and the New Face(book) of Surveillance: Role of Social Media in Reshaping of Contemporary Surveillance.* In T. Dumova and R. Fiordo (Eds.) Handbook of Research on Social Interaction Technologies and Collaboration Software: Concepts and Trends. Hershey, PA: IGI Global.

Becen, Yasin. 2003. "Siber Suçlar", Hukukcu.com October 27 2010, <http://www.hukukcu.com/bilimsel/index.htm >.

Black, Jane. 2004. The perils and promise of online schmoozing. BusinessWeek Online, February 20, 2004. [Accessed 4 November 2010].

Blomley Nicholas K. 1994. *Law, space and the geographies of power.* New York and London: Guilford Press.

Boyd, Danah M. and Nicole B. Ellison. 2008. "Social Network Sites: Definition, History, and Scholarship", *Journal of Computer-Mediated Communication*, 13: 210–230.

Brenner, Susan. "State Cybercrime Legislation in the United States of America: A Survey", November 4 2010, <http://www.richmond.edu/jolt/v7i3/article2.html >.

Burke, Sandra J., Jeff Smith and Ernest A. Kallman. Communications of the ACM, 3 November 2010 < http://cacm.acm.org/opinion/articles >.

Çeken, Hüseyin. Amerika Birlesik Devletlerinde Siber Suçlar", November 3 2010 <http://www.jura.uni-sb.de/turkish/HCeken.html >.

Değirmenci, Olgun. 2002. *Bilişim Suçları*, İstanbul: Unpublished Ph.D. Distertation.

Değirmenci, Olgun and Caner Yenidünya. 2003. *Mukayeseli Hukukta ve Türk Hukukunda Bilşim Suçları,* İstanbul: Legal Yayıncılık.

Donath, Judith S. 1998. *Identity and Deception in the Virtual Community.*In Kollock, P. and Smith, M. eds. Communities in Cyberspace, London: Routledge.

Dülger, Volkan. 2004. *Bilişim Suçları*, Ankara: Seçkin Yayıncılık.

Ellison, Nicole, Rebecca Heino and Jennifer Gibbs. 2006. Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment. October 22 2010, <http://jcmc.indiana.edu/vol11/issue2/ellison.html >.

Erem, Faruk. 1993. *Bilgisayar Suçları ve Türk Ceza Kanunu Şerhi,* Cilt III, Ankara: Seçkin Yayıncılık.

Evans, David C., Samuel D. Gosling and Antony Carroll. 2008. "What elements of an online social networking profile predict target-rater agreement in personality impressions?" Paper presented at the International Conference on Weblogs and Social Media, Seattle: WA. October 22 2010, <http://psychster.com/library/EvansGoslingCarroll_ICWSM08.pdf >.

Findlaw Online, October 12 2010 <Http://blogs.findlaw.com/law_and_life/2009/07/amanda-bonnen-and-the-50k-tweet.html>.

Gandy, Oscar H. 2002. "Data mining and surveillance", In the Post-9.11 Environment. Paper presented at the annual meeting of the IAMCR, Barcelona,

Spain. October 22 2010. < http://www.asc.upenn.edu/usr/ogandy/IAMCRdatamining.pdf >.

Gross, Ralph and Alessandro Acquisti. 2005. "Information Revelation and Privacy in Online Social Networks (The Facebook case) Pre-proceedings version." Heinz.cmu.edu. October 22 2010. <http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf> .

Herring, Susan C. and Anna Martinson. 2004. "Assessing gender authenticity in computer-mediated language use: Evidence from an identity game", *Journal of Language and Social Psychology* 23 (4), 424-446.

Hoar, Sean B. 2001. "Identity Theft: The Crime Of The New Millennium", October 22 2010. < http://www.justice.gov/criminal/cybercrime/usamarch2001_3.htm [Acces22 October 2010].

H. R. 2006. Deleting Online Predators Act of 2006. H.R. 5319, 109th Congress. Retrieved July 21, 2007, Govtrack.us. October 22 2010. <http://www.govtrack.us/congress/billtext.xpd?bill=h109-5319 >.

Huffington Post Online, October 14 2010 <http://www.huffingtonpost.com/2010/01/20/amanda-bonnen-twitter-sui_n_430522.html> .

Huffington Post Online, October 14 2010 < http://www.huffingtonpost.com/gregory-gabriel/to-defame-or-not-to-defam_b_445171.html>.

Jacobson, David. 1999." Impression formation in cyberspace: Online expectations and offline experiences in text-based virtual communities". *Journal of Computer-*

Mediated Communication, 5(1). October 22 2010,

<http://www.ascusc.org/jcmc/vol5/issue1/jacobson.html>.

Karagülmez, Ali. 2005. *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*, Ankara: Seçkin Yayıncılık.

Katyal, N. Kumar. "Criminal Law in Cyberspace", SSRNEL, October 23 2010,

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=249030 >.

Kurt, Levent. 2005. *Açıklamalı ve İçtihatlı Tüm Yönleriyle Bilisim Suçları ve Türk Ceza Kanunundaki Uygulaması,* Ankara: Seçkin Yayınevi.

Lee, Eun-Ju. 2006. "When and how does depersonalization increase conformity to group norms in computer mediated communication?", *Communication Research* 33, 423-447.

Mahmutoğlu, F. Selami. 2001. *Karşılastırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu,* İstanbul: Kazancı Hukuk Yayınevi.

Meyrowitz, Joshua. 1986. *No Sense of Place,* New York: Oxford University Press.

Miah, Andy. 2000. "Virtually nothing: re-evaluating the significance of cyberspace", *Leisure Studies*, 19, 211-225. Anchor/Doubleday.

Odabaşı, Arda. 1999. *Bilgi Toplumu mu, Gözetim Toplumu mu?,* İstanbul: Bilim ve Ütopya.

Önder, Ayhan. 1994. *Şahıslara ve Mala Kasti Cürümler ve Bilişim Alanında Suçlar,* İstanbul: Filiz Kitabevi.

Özdilek, A. Osman. 2002. “Bilgisayar Suçları Ne Kadar Ciddi”, October 23 2010, http://www.hukukcu.com/bilimsel/kitaplar/bilgisayar_suçları.html >.

Özel, Cevat. 2001. “Bilişim Suçları ile İletişim Faaliyetleri Yönünden TCK Tasarısı”,İBD, C: LXXV, October 23 2010, <http://www.dulger.av.tr/assets/pdf/bilisimsuclariveyctk.pdf>.

Özel, Cevat. 2002. “Bilişim-İnternet Suçları”. October 23 2010, <http://hukukcu.com/modules/smartsection/item.php?itemid=74>.

Özgenç, İzzet. 2005. *Türk Ceza Kanunu Gazi Şerhi, Genel Hükümler,* Ankara: Seçkin Yayıncılık.

Özgenç, İzzet and Cumhur Şahin. 2001. *Uygulamalı Ceza Hukuku,* Ankara: Seçkin Yayıncılık.

Popescu, Mihaela and Lemi Baruh. "Captive audiences and unwanted advertisement: The construction of public/private borders in legal discourse",October 23 2010. <http://www.allacademic.com/meta/p111439_index.html >.

Schjolberg, Stein. “The Legal Framework – Unauthorized Access to Computer Systems; Penal Legislation in 44 Countries”. October 20 2010. <http://www.mosstingrett.no/info/legal.html >.

Schuster, Bernard and Patricia Wallace. 1995. *The Psychology of the Internet,* Cambridge: Cambridge University Press.

Sınar, Hasan. 2004. *Avrupa Konseyi Siber Suç Sözlesmesi Üzerine Bir Deneme,* İstanbul: Galatasaray Üniversitesi Yayınları.

Sınar, Hasan. 2001. *İnternet ve Ceza Hukuku,* İstanbul: Beta Basım Yayın.

Sınar, Hasan. 1997–1998. *İnternetin Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı,* İstanbul: MHB.

Smith, H. Jeff. 1994. *Managing Privacy: Information Technology and Corporate America.* Chapel Hill, NC: University of North Carolina Press.

Solove, Daniel J. 2007. *The future of reputation: Gossip, rumor, and privacy on the Internet,* New Haven, CT: Yale University Press.

Stone, Eugene F., Donald G. Gardner and Hal G. Gueutal. 1983. "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations", *Journal of Applied Psychology*, 68: 459 - 68.

Sundar, S. Shyam, Sunetra Narayan and Rafael Obregon. 1998. "Does web advertising work? Memory for print vs. online media", *Journalism and Mass Communication Quarterly, Winter 1998*, 822-35.

Turkle, Sherry. 1999. *Life on the Screen: Identity in the age of the Internet.* New York, NY: Touchstone.

Üçel, Kayıhan., İzzet Özgenç and Adem Sözüer. 2000. *Suç Teorisi,* İstanbul: TURDAV.

Ünver, Yener. 2001. *Ceza Kanununun Değerlendirilmesi*, İstanbul: İÜHFM.

Walther, Joseph B. 1996. "Computer-mediated communication: Impersonal, interpersonal, and hyper-personal interaction", *Communication Research*. February 1996 vol. 23 no. 1 3-43.

Walther, Joseph B. 2007. "Selective self-presentation in computer-mediated communication: Hyper-personal dimensions of technology, language, and cognition", *Computers in Human Behavior*, Volume 23, Issue 5, September 2007, Pages 2538-2557.

Walther, Joseph B, Celeste Slovacek and Lisa C.Tidwell. 2001. "Is a picture worth a thousand words? Photographic images in long term and short term virtual teams", *Communication Research,* February 2001 vol. 28 no. 1 105-134.

Walther, Joseph B. and Malcolm R.Parks. 2002. *Cues filtered out, cues filtered in: Computer-mediated communication and relationships*, In Handbook of interpersonal communication, 3rd ed., M.L. Knapp and J.A. Daly, Eds. Sage Publications, Thousand Oaks.

Walther, Joseph B, Brandon Van Der Heide and Kim Sang-Yeon. "The Role of Friends' Appearance and Behavior on Evaluations of Individuals on Facebook: Are We Known by the Company We Keep?" *Human Communication Research,* Vol. 34, No. 1. (2008), 28-49.

Weintraub, Jeff. 1997. "Public/Private: The Limitations of a Grand Dichotomy", *The Responsive Community* 7:2, pp. 13-24.

Westin, Alan. 1967. *Privacy and Freedom,* New York: Atheneum.

Yamaç, Fatih, Semih Dokurer and Mehmet Özcan. "Bilişim Suçları" , October 20 2010, < http://inet-tr.org.tr/inetconf7/bildiriler/86.doc >.

Yazıcıoğlu, Yılmaz. 1997. *Bilgisayar Suçları, Krimonolojik Sosyolojik ve Hukuki Boyutları ile*, İstanbul:Alfa Basım Yayın.

Yee, Nick. 2009. "The Proteus Effect Implications of Transformed Digital Self-Representation on Online and Offline Behavior." October 10 2010. <http://crx.sagepub.com/cgi/content/abstract/36/2/285>.

Zarsky,Tal Z. 2002. "'Mine Your Own Business!'" Making the case for the implications of the data mining of personal information in the forum of public opinion" Yale Journal of Law and Technology, volume 5. Yjolt.com. August 10 2010. < http://www.yjolt.org/files/zarsky-5-YJOLT-1.pdf>.

Zizi, Papacharissi. 2009. "The virtual geographies of social networks: a comparative analysis of Facebook, LinkedIn and AsmallWorld", *New Media Society,* February/March 2009 vol. 11 no. 1-2 199-220.