THE CONCEPT OF INFORMATION TECHNOLOGY IN TURKISH LEGISLATION WITHIN THE CONTEXT OF TURKEY'S ACCESSION TO THE EU

Özhan TINGÖY*

Abstract

The introduction of information technologies into society has played a part in the world becoming smaller and smaller. As a result of the rapid development, diffusion and use of information technologies, a number of issues and new kind of offences have arisen in practise. In addition to these issues and offences, new concepts such as the information society, cyberspace and information offences have emerged. International co-operation is being conducted between states in combating these new types of offences. Member states of the Council of Europe signed a Convention on Cybercrimes in Budapest on 23 Nov. 2001. The convention on Cybercrimes is very important, since it is the first convention providing for international co-operation. In Turkey, on 14 June 1991, "Chapter 11" entitled "Crimes in the Information Area" was added following after Article 525 in the Turkish Penal Code and, thus, crimes committed in the information area have been arranged as independent and separate offences. In this study, examples of cybercrime, which are increasingly dependently on the rapid diffusion of information technologies in Turkey, have been examined in accordance with the Turkish Penal Code and it has been suggested that e-laws appropriate to information technologies must be made in the process of accession to the EU.

1. Introduction

The diffusion of Information Technologies throughout the world is encroaching on the lives of people each hour of the day at a remarkable pace

* Assistant Professor, Marmara University, Faculty of Communications

and with increasingly new applications. The development of information technologies is continuously expanding. Within this development, the production, distribution, and exchange of knowledge are of vital importance. Moreover, information technologies are creating considerable changes in every area of life. Information requires that knowledge has to be produced, exchanged mutually and interactively. Information therefore, involves sharing, participation and transparency. Consequently, information rejects the unacceptable, the incorrect, the inaccurate and the libellous and easily distinguishes between such detrimental information.[1] As a result, information technologies have caused many changes in society and at the end a new form of society has emerged. An important change has become necessary in legislation. Along with those changes, offences are changing accordingly.[2]

The integration of communication and information technologies enables distances to become ever shorter. Thus, people are able to communicate with each other wherever they are in the world. A variety of criminal offences are being committed by misusing information technologies and media networks and this type of criminal activity is known as cybercrime.

In order to reach comprehensive conventions in the fight against cybercrime, intensive international studies are being carried out. In addition, the member states of the Council of Europe are working to achieve a common criminal policy based on international co-operation that involves adopting a single legislation and applying a common criminal enforcement.

Studies relating to cybercrime were initiated by taking into consideration the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms and, the 1966 United Nations International Covenant on Civil and Political Rights and other international human rights treaties. The concept of information crime was described in the 1981 Council of Europe Convention for the Protection of individuals with Regard to Automatic Processing of Personal Data. In 1989, the OECD and European Committee on Crime Problems proposed that the application of information technology crime should be made in accordance with the legal systems and traditions of each individual country. In Nov 1966, the European Committee on Criminal Problems formed an expert committee on cybercrimes. In 1997, this committee prepared a legal text relating to subjects including cybercrime. On account of the rapid development of communication and information technologies, the Council of Europe's

Convention on Cybercrime (Budapest, 23 Nov 2001) agreed a common policy of punishment in order to ensure international co-operation among the 26 member states of the Council of Europe and the other non-member States (USA, Japan, Canada and South Africa) and, to protect society and the individuals against Cybercrime in accordance with legislation and to provide coordination in conventions for prosecution.

In this paper, the description of information offences in Turkish Law and their historical development and the Convention on Cybercrime of Council of Europe will be considered. Examples pertaining to decisions of the Turkish Supreme Court will also be examined.

2. Information

Information, to be useful, must be accurate, timely, complete, verifiable, and consistent.[3] Raw facts and figures constitute data. Facts and figures often have little meaning until they are sorted or until one is able to calculate something from them. This sorting or calculation is known as processing. When data is processed it provides information.

Information concerns the meaning we attach to the data. For instance, a red traffic light is a form of data. The meaning we attach to this data (STOP) is the information. Sometimes data can give rise to ambiguous information. If one is driving a car and a car travelling in the opposite direction flashes its lights at you, what does it mean? It could just mean that a friend has spotted you and wants to say hello or; it could also mean that there is an accident further up the road.

The information that may be obtained from data depends on the way that the data is interpreted and the context in which it is used.[4]

3. Information Offence

Information and communication technologies are developing rapidly and becoming increasingly widespread today. The Internet plays a major role in the development of these technologies. In this age of globalization, the use of the Internet by individuals or institutions is at the utmost level. Accordingly, offences committed in

the information area are also increasing parallel with this development and, thus, threaten individuals or institutional users.

The development of information and communication technologies is impacting societies in many aspects. Frankly speaking, information has taken individuals and institutions under its control. Due to continuous change and development in information technologies, existing legislation has become inadequate. Technology is changing at such a pace that even while it is being used it may be out of date. In spite of the positive effects of the developments in information and communication technologies, changes in social rules and new kind of offences represent the negative side to the use of technologies. Together with the development of technology, social values such as responsibility, personal rights, security, honesty, confidentiality and property rights are also being affected.

Information offences resemble other offences. Information offences include, together with information and communication facilities, satellites, telephone lines, multimedia hardware and immobile devices. Thus information offences have spread across a very wide area.

When the historical development of information offences is examined, it can be seen that computer viruses form the first examples of information offences. The problem of computer virus appeared for the first time in 1983. Computer viruses alter or damage the sources of the computer. Viruses alter software, reproduce themselves, developing harmfully damage the data and spread throughout the hardware. Ultimately, viruses completely suppress the entire function of computer systems.

The concept of information offence has also been extended with the diffusion of the Internet. Communication possibilities have played a major role in this expansion. For instance, technologies such as wired and wireless communications units, which contain telephone lines, microwaves, satellites and GSM, are connected to computer or computer systems.

The principal forms of information offence, currently existing, are as follows:

- Unlawful acts of intrusion of telephone networks

- Infringement of integrity of networks
- Privacy violation
- Industrial espionage
- Infringements of copyright of computer software
- Fraud
- Abuse of the Internet
- Committing criminal offences such as homicide, terrorism, child pornography, aggression to the Internet, by using computers or information technologies
- Assault on computers with multimedia hardware
- Assault on software
- Data storage attack.[5]

4. Historical Development of Information Offences in Turkish Law

Prior to Act No.3756 (This chapter and caption, was affixed to the text with Article 20 of the Act of 6 June 1991) there was a wide gap in the Turkish Penal Code with regard to information offences. Acts in such areas were evaluated according to traditional types of offences, such as theft, fraud and causing damage.

These offences will now be examined in more detail,

Theft

If Articles 525/a-c of the Turkish Penal Code did not exist, gaining access to data would not be taken under sanction with Article 491/1[6] of the Turkish Penal Code, because the subject of theft offences in law is movable property. Thus, data and information obtained from an information system cannot be considered to fall under this description.

Forgery

Although, acts such as breaking and damaging one part of a system, which are in Article 525/b of the Turkish Penal Code, might be considered in Article 516[7] of Turkish Penal Code, other acts such as deleting all data,[8] and causing to operate incorrectly cannot be introduced into the same Article 516.

Swindling

Due to the fact that the injured party of the fraudulent act ought to be a real person, fraudulent actions executed against a machine cannot be[9] thought of in terms of Article 503.[10]

In general, as the elements of offence do not coincide with each other, this might result in flawed applications or that actions not covered by law, remain unpunished as well since criminal law is based on the principle that "offence and punishment do not happen without law". This is an accepted principle; which means that, in cases where no judgment exists openly in law, offence and punishment cannot be established only by interpretation of judgments existing in law. A judge doesn't have the authority to create offence and punishment.

In accordance with Article No: 1 of the Turkish Penal Code "nobody will be punished for an act which is not accepted openly as an offence by law". And nobody will be punished with a penalty other than that contained in law. In other words, the rule of becoming lawful in offence and punishment is a universal legal provision and this is the first Article of the Turkish Penal Code.

Further, according to the second Article of The Turkish Penal Code, "Nobody can be punished for an act that is not accepted as a misdemeanour or crime with respect to the law on the date when it is committed. Nobody can also be punished for an act, which is not accepted as a misdemeanour, or crime with respect to the law made after the act is committed. If such a punishment, its execution and legal consequences will self - invalidating. In such a situation, in accordance with the rule of legality in offence and punishment, punishment cannot be given owing to an offence, which has not been defined and stipulated by law.[11]

For these reasons, Parliament has defined the offences committed in the information area as an independent and distinct offence and appended these as "Chapter Eleven" under the heading of "Offences in Information Area" to Article 20 of Act 3756 of 14 June 1991 together with Article 525 of the Turkish Penal Code.

As for the legal motives underlying this move, legislator has explained "it was necessary to bring those judgments (in the Chapter) to protect the installed program, data and all other elements with great sensitivity, because information technologies have spread widely in contemporary life very quickly".

The term of "Offences in the Information Area" in "Chapter Eleven" added to the Turkish Penal Code describes not only computer offences but also the acts of obtaining useful information with the help of computer during data storage and processes, or similar acts relating to computer offences.

5. Offences in the Information Area in Turkish Penal Code

5.1. Turkish Penal Code "Chapter Eleven (2)"

Offences in Information Area: Article 525/a

A person who gains access to programs, data or any other element illegally from a system processing data automatically will be sentenced from one year to three years in prison with a further heavy fine of between one million and fifteen million TL.

A person who transfers and reproduces a program, data or any other element existing in a system, which processes data automatically for the purposes of damaging to someone else will also be sentenced to the same punishment contained in the Article above.

Damage to System and Data: Article 525/b

A person who damages or modifies or deletes an automatic data processing system, or data or any other element completely or partly; or hinders the operation of the system or causes system damage to someone

else, or to derive benefit for himself or an other person, will be sentenced from two years to six years in prison with a further heavy fine of between five million and fifty millionTL.

A person will be sentenced from one year to five years in prison with a further heavy fine of between two million to twenty million lira for attempting to secure benefit illegally for himself or other person by using an automatically data processing system.

Alteration of Evidence: Article 525/c

A person who puts data or other elements into a system processing data automatically or alters fraudulently the existing data and other elements in order to constitute a fake document for the purpose of using it as evidence in legal area, will be sentenced to a prison one year three years and persons who use these altered data on purpose will be sentenced to a prison term of between six month and two years.

Prohibiting From Occupation and Craft: Article 525/d

Those persons who breach the judgments of Article 525/a and 525/b will be prohibited from practising their occupations, crafts or trading or from practising public service in which an offence has been committed while carrying it out, or on account of carrying it out, from six months to three years in addition to the punishments contained in the above Articles.[12]

6. The European Union and Cybercrime

There is clearly a need to ensure a carefully considered balance between the demands of law enforcement and respect for fundamental human rights, as designated in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, other international human rights treaties, which reaffirm the right of everyone to hold opinions without being under any influence, the right to freedom of expression, including freedom to seek, receive and transmit information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy.

The fundamentals of the concept of cybercrime have been established by taking into account the intent of the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and giving the necessary importance to this subject, In 1989, the OECD and European Committee on Crime Problems have recommended that the application of cybercrime should be considered under the domestic law of individual states and with regard to the traditions of each country. The widespread using of information and communication technologies, has created a media known as cyberspace. This space can be used for legal objectives as well as illegal ones. In view of this situation, the European Committee on Crime Problems adopted Resolution No. 103-211196 in Nov 1996 to establish a Committee consisting of Experts concerned with cybercrimes. Cybercrimes can be committed against the integrity, confidentiality and availability of computer systems and communication networks, as well as playing a role in the execution of traditional crimes. This committee prepared a text in 1997, which is of a legal nature and concerned with the subjects covering cybercrime. This text constitutes the fundamental principles of the first international convention on cybercrime. Based on the studies mentioned above, considering the necessity for providing legislation, coordination convention on judging, and developing international co-operation in order to protect society and individuals against cybercrime by criminal law provision, the Council of Europe, established a common criminal policy by Convention on Cybercrime in Budapest on 23 Nov 2001.

6.1. The Convention on Cybercrime of the Council Of Europe

The convention on cybercrime of the Council of Europe was signed in Budapest on 23rd November, 2001 by 30 states consisting of 26 member states of Europe and the USA, Japan, Canada and South Africa. This important convention is the first accepted document to provide for international cooperation against cybercrime in a global context[13].

This convention was signed following the work of a two-year commission and sub-commission study. Turkey was unable to participate in this extensive study.

The convention on cybercrime of the Council of Europe has been written in such a way that it may be enlarged by protocols at a later time in order to cover new cybercrimes, likely to appear in the future. The

Convention on Cybercrime of the Council of Europe has three main objectives.

The main objectives of the convention on cybercrime are as follows:

- To establish common definitions concerning the crimes connected with the use of new technologies

- Definition of means of investigations concerning data storage, search of communication data, collection and seizure and communication authority
- Definition of methods of international co-operation.

Definition Pertaining to Offences in the Convention:

- Offences directed against the confidentiality, integrity and availability of computer data and computer systems (virus distribution, access to company confidentiality)

- Offences related to computer (virtual forgery and fraud offences)

- Offences related to content (procuring child pornography and distributing it at an international Level)

- Offences related to the infringement of intellectual property rights (USA Act of Anti-Terror)

The Convention consist of four main chapters (definitions, measures to be taken at the national level, international co-operation and final provision), in which chapters are infringement of copyright, computer-related actions of forgery, child pornography, infringement of security of network, the authority and procedures to be used for combating cybercrimes.

The Preamble of Articles in the Convention on Cybercrime is given in the followings:

Computer system, computer data, service provider and traffic data are defined in Article 1 of the Convention. These definitions are very important

from the view of the effective application and interpretation of Articles in the Convention. With Articles 2-13 of the Convention, offences are specified. Such an adoption must be realized both at the national and international level. It is, therefore, considered important to support international co-operation. This chapter consists of five titles. Title 1 contains fundamental offences (confidentiality, integrity, computer data and threats directed against the availability of computer data) related to computers. Titles 2, 3, and 4 cover the other offences related to computers. Action proceeds in these offences; computer and communication systems are used for the purpose of aggression upon benefits, which are under the protection of criminal law. Computer-related forgery and fraud is dealt with in Title 2; Title 3 covers the actions directed against producing child pornography for the purpose of its distribution through a computer system without right. Considering these offences, the committee preparing the outlines of the text discussed the distribution of racist material by computer systems, but couldn't reach a definitive solution and agreed on placing the matter in a supplementary protocol. Offences related to infringement of copyright and related rights are in Title4. Infringements of copyright are being experienced considerably in the offences relating to computers and have an international bearing. Title 5 covers sanctions directed against aiding, attempt or abetting the commission of any of the offences. Provisions in Article 14-21 cover the measures to be taken at the national level for the purposes of investigations concerning criminal offences stipulated in the convention; other criminal offences related to computer systems and the collection of evidence in electronic form of a criminal offence. Article 22 determines the rules of jurisdiction to be applied to the member states when an offence is committed. Article 23 includes the general principles relating to international co-operation. According to this article, the parties shall develop forms of co-operation with each other avoid applications, which will hinder the flow of information. The co-operation under consideration shall include all kinds of offences related to the computer systems and computer data. The co-operation to be developed ought to be in harmony with the rules in the conventions. Article 24 includes the provisions connected with extradition within the framework of international co-operation; Article 25 includes general principles relating to mutual assistance; Article 26 includes the principles that a Party may forward to another party of valuable information that might assist the receiving Party in carrying out investigations. As for Article 27 and 28, those include procedures pertaining to requests of mutual assistance in the absence of applicable international convention.[14]

7. Examples of Supreme Court Decisions Relating to Information Offences Committed in Turkey

7.1. Case 1

In 1997, a visually impaired person fell into a hole, being dug by workmen from the Greater Ankara Municipality Council and was injured. His visually impaired friends gathered together in order to protest against the irresponsibility of the Municipality, but they were beaten with clubs.

Films, photographs and articles pertaining to the incident were broadcast on TV and published in the newspapers. A user of one Internet Service Provider, who had followed the incident from the press, wrote his views relating to the incident on his Internet form page. Another user reading this message expressed his worries concerning the event and accused 'the security forces' on his daily forum page. A further person read the published message and took a printout of it, then informed on the person was the security forces. As a result of the public law suit, the offender complaining about the behaviour of sentenced to 10 months in prison for violation of Article 159/1[15] of the Turkish Penal Code. On consideration of his good behaviour, penalty was quashed.

As a result of this incident and the ensuing of conviction, a message published on the Internet has been classed as a criminal offence for the first time in Turkey [16]

7.2. Case 2

An Internet Service Provider opened a free forum of debate on the Internet at the request of his subscribers. The subject of debate, on 26 May 1999, was "Violations of Human Rights in Turkey". A subscriber reading the message sent to the free forum of debate by someone using the symbol (a man), sent a reply requesting that the message must be deleted immediately from the page, because its content constituted a criminal offence. The newspaperman who worked at the Service Provider as a coordinator of the interactive departments related to broadcasting on the Internet didn't consider the request important and the writing was not deleted. Consequently, the person who requested the deletion and saw that his request had been ignored complained to the Minister of Justice about the newspaperman, whom he considered responsible for the material published

on the Internet. The incident became a matter in dispute and was transferred to the office of the prosecutor. The Istanbul Penal Court issued a judgment of 40-month imprisonment the guilty person on 27 March 2001; decision no. E.1999/225, K.2001/56. The judgment (E.1999/225, K.2001/56 and 27 March 2001) of 40 months heavy imprisonment for the guilty person of Istanbul Penal Court No.4 was transferred to the Court of Appeal.

The decision of 4th Civil Law Section of Court of Appeal numbered E.2002/755, K.2001/1157, which is dated 8 Feb 2001 and, was issued under the following title: aggression to personal rights by way of press, moral compensation and stopping the broadcasting on the Internet. The matter in dispute is connected with the requests for moral compensation and also stopping the broadcast of the massage in the Internet, which arose as a result of aggression to the personal rights by way of press. The law court accepted the request for moral compensation partly and decided; also "to stop broadcasting the message on the Internet." The decision made clear that there is not yet any legal arrangement regarding to the procedure to be implemented in respect to the broadcasting on the Internet. To be able to realize the binding force of the court decisions, the judgment has to be executable and so its sanction ought to be applied. At this stage, there was not any legal arrangement for removing or stopping a broadcasting being transmitted, including ones transmitted on the Internet. Consequently, the judgment of acceptance of request connected with the above has been the cause of annulment. The moral compensation amount is estimated according to the characteristics of the act and the event constituting the cause of aggression, as well as degree of negligency, title, position occupied, and other social and economic situations of the parties. The money to be awarded should possess a special quality, which will balance the losses of the person who is being aggrieved. The limit of compensation should be limited according to its objective.[17]

Attributing this decision of 4th Law Division, 9th Penal Division with its decision on 14.Nov.2001 the judgment of 40 months imprisonment for the newspaperman for the writing published on a WEB page, was overturned and the suit was remanded for further proceedings.

With respect to the decision dated 25.Oct.2001 and no.E.2001/1854, K.2001/2649, of the 9th Division of the Supreme Court, the statement of reasons for the overturning of sentence was as follows:

- In the first place, investigation has to be conducted into what position the accused has in the mentioned company, whether he has the official duty and authority to interfere with the material subject to the incrimination, which are sent to the forum by e-mal in the Internet media and whom the authority, belongs to.

- Following establishment of the above an expert in the Internet will enquire as to whether the Superonline Company is an Internet Service Provider (ISP), or an access provider or both; and that, in the event of it being an ISP, who is the owner and that whether the forum and WEB site system, in which material subject to prosecution has been published on the Internet, belongs to another firm; and, while it is necessary to appreciate the situation of the accused, taking into account the above mentioned consideration to make a decision with incomplete investigation is unlawful and, therefore, the 9th Division of Supreme Court has decided the overturning of the judgment[18].

8. Conclusion

As a result of the fast development and spread of technologies in the world, information technologies have also entered into the sphere of social life. The use of information technologies is also developing and spreading with an amazing speed in Turkey and, thus, new kind of offences are becoming current issues in practice. These threats (offences) will continue in the future. Thus, an effective legal strategy against information offences should be prepared. These strategies should be developed and new legal arrangements should be put in place. The principle cause of this is the transformation of information offence into cybercrime caused by the development of distributed multimedia in the information sector.

Prior to Act 3756 there was a deficiency relating to information offences. Acts in this area were being evaluated as classical type of offences such as theft swindling and criminal damage. In determining the principles, which will be dominant in establishing the relationship between the criminal law having the hardest discipline of public law and information, extreme carefulness should be exercised.[19] The fact that criminal law as a branch of law determines the limits of freedoms in a way and that, on the other hand, information provides an environment in which telecommunication is being used unlimitedly, requires a proper balance between the demands of criminal law and information.

Information technologies have been extended over a wide are from distributed multimedia to the wireless communication. However, states are struggling to prepare a common law concerning the offence. The Council of Europe, with the Cybercrime Convention signed in Budapest on 23.Nov.2001, has made legal arrangements for the protection of the individual and society against cybercrime. The main objective of Turkey in combating cybercrimes must be to make legal arrangements aimed at the creation of societies based on the use of information technologies, human rights and freedoms at the utmost level, adopting the supremacy of law, and the pluralist and participating democracy of a changing society. While achieving this objective, Turkey must act in accordance with the Council of Europe Convention on Cybercrime. In Turkey, the existing laws must also be arranged and applied as e-laws in accordance with the Council of Europe Convention on Cybercrime.

Endnotes

[1] Halıcı Emrehan, Bilgi Toplumuna doğru, Türkiye Bilişim Şurası Sonuç Raporu, 10-12 Mayıs 2002, s. IX.

[2] Sezer, N. Ahmet, Bilgi Toplumuna doğru, Türkiye Bilişim Şurası Sonuç Raporu, 10-12 Mayıs 2002, s. V.

[3] Blyth, A., Kovacich, G.L., Information Assurance, Springer, 2001, p. 29.

[4] Doyle, Stephan, Information Systems: for You, Stanley Publishers, 1995, pp: 6-8.

[5] Kizza J., M., Ethical and Social Issues in the Information Age, Springer, 2003, pp. 240-241.

[6] Whoever takes the other's movable property from where it is placed without his consent in order to make use of it is to be imprisoned from six months to three years. Every kind of energy source, which has an economic value, is also regarded as movable property.

[7] If somebody destroys or eliminates or impairs or damages, in any way whatsoever, the other's movable or immovable property, he will be sentenced, on complaint of the person who suffers loss, to prison from one year to three years with a further heavy fine from one thousand to three thousand Turkish lira.

[8] Çetin Erol, Malkoç İsmail, Uygulamada Sahtekarlık suçları, Bilgisayar Suçları,Tebligat Suçları ve İlgili Mevzuat, Adalet Yayınevi, Ankara, 1995, ss. 543-545.

[9] Taşdemir Kubilay, Bilişim Suçları Paneli,Uygulamada Bilişim Suçları 28 Şubat 2001, Adalet Bakanlığı Hakim Savcı Adayları Eğitim Merkezi Başkanlığı, Ankara Açık Cezaevi Matbaası, 2001, ss. 42-50.

[10] If a person, by engaging in deceitful behaviour and fraud tricks and frauds, misleads somebody and causes him or other's loss and derives benefit unjustly for himself or the other is to be sentenced to from one year to three years in prison with a further heavy fine of the benefit he got and the same sum again. Concerning the person who commits the fraudulent act, by making use of the fault which exists essentially in the injured one, it the same punishment written in the first paragraph is to be applied.

[11] İlkiz Fikret, İnternet Ortamındaki Yayınlarda iki olay ve iki mahkumiyet kararı ve yasal Çalışmalar, İstanbul Barosu Dergisi, Sayı: 4, Aralık 2001, ss. 1017-1021.

[12] This chapter and caption, has been affixed to the text with Article 20 of the Act of 6 June 1991 and No. 3756.

[13] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[14] www.turk.internet.com

[15] Those who insult and ridicule publicly the Turkish ness, the Republic of Turkey, the Turkish Grand National Assembly, the Moral Personality of Government, Ministries, Military or Police Security Forces or Moral Personality of Justice are to be punished from one year to 6 years by imprisonment.

[16] İlkiz Fikret, İnternet Ortamındaki olaylarda İki olay ve İki Mahkumiyet Kararı ve Yasal Çalışmalar, İstanbul Barosu Dergisi, Sayı:4, Aralık 2001, ss. 986-987.

[17] Yargıtay Kararlar Dergisi, cilt.27, sayı.7, temmuz 2001, ss. 994-996.

[18] İlkiz Fikret, İnternet Ortamındaki olaylarda İki olay ve İki Mahkumiyet Kararı ve Yasal Çalışmalar, İstanbul Barosu Dergisi, Sayı:4, Aralık 2001, ss.987-988.

[19] Türkiye Bilişim Şurası Sonuç Bildirisi, Türkiye Bilişim Şurası Sonuç Raporu, 10-12 Mayıs 2002, s. 369.