A RESEARCH ON INFORMATION TECHNOLOGIES CRIMES IN THE TRNC SECONDARY SCHOOLS DISCIPLINE DIRECTIVE

Ali Çoban
alicobanppl@gmail.com
https://orcid.org/0000-0001-9411-4188
TRNC Ministry of National Education, Department of Secondary Education Teacher

Aytaç Küçük
aytackucuk1980@hotmail.com
TRNC Ministry of National Education, Department of Primary Education TECHER
https://orcid.org/0000-0002-8639-9096

Peyda Çoban
Peyda1981@gmail.com
TRNC Ministry of National Education
https://orcid.org/0000-0002-9850-0569

ABSTRACT

"Rules and Disciplinary Regulations to be followed in and out of Secondary Schools and Secondary Education Institutions" has been observed that the regulation named, which was last renewed in 1989, is not suitable for today's conditions. With the advancement of technology, many new crimes that have not been defined have emerged. In order to combat cybercrime in schools, it is necessary to amend the statute and determine new articles on "Information Technologies Crimes". In the transition process of countries to information society, the use of information technologies becomes an integral part of life. In this process, society uses more information technology and inevitably more cyber crimes are encountered. Many security problems occur with the use of information technologies in all areas of life. For this reason, it has become an important issue for students to use information technologies safely. Schools are going through a similar process as a part of technological development and transformation into an information society in the TRNC. For this reason, it is necessary to include additional clauses in the disciplinary regulations in order to ensure the safety of everyone, as well as to use technology without being behind the times.
Keywords: Secondary Schools, Disciplinary Regulations, IT crimes; IT Law

INTRODUCTION

Discipline

The meaning of the Latin word discipline is to learn, to teach; its educational meaning is to train people to achieve self-control. It is assumed that when people reach self-control, they can direct their behavior in accordance with social and moral rules without the need for discipline. Başaran (2006) defines discipline as "the sanction system established to ensure the adaptation of students to school". According to Başaran, aim of the discipline; to teach students the rules of behavior that must be followed at school, to monitor whether the students behave in accordance with these rules, to reward those who turn appropriate behavior into a habit, and to punish those who turn violations into a habit. According to this definition, discipline is a learning process. The disciplinary system is the judicial order of the organization. In fact that people who behave in violation of the principles and rules comply with discipline (Başaran, 2006). In daily life, the word "discipline" is generally used to mean the rules and order of a group or an organization; this is also called ensuring discipline or providing discipline. On the other hand, discipline describes the situation where there are various people who will be affected by this situation. As a general result, the discipline;
- for appropriate behavior individual's self-monitoring.
- to establishment and maintenance of regularity in an organization individuals show appropriate behavior.
- to take necessary precautions for individuals to show appropriate behaviors and correcting misbehavior.

Discipline is a term often used by practitioners and members of the school community. However, there is no clear agreement on the meaning of the concept of discipline. Because during the implementation, the values and beliefs of the school community are effective. School discipline is defined as the student's behavior in accordance with the school regularity, taking the necessary precautions and making arrangements (Sarpkaya, 2005). Discipline is a sanction system prepared to ensure order and peace in the school and to prepare an environment suitable for the smooth functioning of education. In this direction, after the students are told what

behaviors they should not engage in, the behaviors of the students can be kept under control so that undisciplined behaviors can be punished. The main purpose is not to punish the student, but to create a deterrent environment for undesirable behaviors. Behaviors against discipline are listed in the first part of the third section of the Ministry of National Education Secondary Education Institutions Award and Disciplinary Regulations and the penalties corresponding to these behaviors are specified (Erkesici, 2005).

Discipline, defined as the dominance of laws and regulations in the community, is one of the necessary elements for the continuation of education and training. Although it is not possible to talk about an undisciplined education; it is not possible for effective teaching to take place with extremely oppressive discipline practices. Disciplinary practices in educational institutions have been discussed from the past to the present and appropriate discipline models for effective education have been researched (Şengül, 2005). Charles (2002) defines discipline as what is done in schools to help students behave appropriately. Charles defines effective discipline as helping the student demonstrate appropriate behavior while maintaining good relationships and maintaining volunteerism for cooperation. The concepts of discipline and punishment are often used synonymously with each other and sometimes interchangeably. However, these two concepts differ significantly from each other. Punishment is a reaction to undesirable or harmful behavior. Discipline, on the other hand, includes the measures to be taken before, when or after the problems related to the undesired behavior occur and the processes related to the actions taken (Çelik, 2008).

Information Technologies and Internet

Information Technologies is basically the theoretical infrastructure of computation and knowledge. It is the science that deals with the application and establishment of knowledge and computation with practical techniques. In other words; it is the practice of processing information with technological devices such as computers.

The Internet is made up of the words Inter (between) and net (network). This means "inter networks". The Internet is characterized as a communication network that is independent of all restrictions and borders, functions outside of central control and allows computers to be connected to each other within a network. In short, the internet is characterized as an electronic communication network that enables computer networks to be connected to each other by using a transfer control protocol called TCP/IP. The meaning of the Internet in Turkish is specified as the general network. Its exact equivalent in English is defined as a set of interconnected networks. For this reason, it is derived from the English word "interconnected networks".

The Internet makes access to information accessible worldwide. Regardless of the location, information can be shared and communicated easily. It allows all devices with a system called Internet TCP/IP to connect to each other. The Internet works on the same principles as telephone lines, which are connected with each other in a way. In many parts of the world, the internet continues to function over telephone lines that are still available. There are terrestrial lines interwoven between countries. In addition, fiber cables and satellite infrastructure are laid under the ocean. Thanks to these lines, countries are connected to each other with the internet network and communication is possible. Thanks to the Internet, information can be easily accessed at any time, regardless of location.

Information Technologies (IT) Crimes

IT crimes, in other words cybercrime; It can be defined as all kinds of crimes committed in electronic environment by using modern communication tools such as computers, tablets, mobile phones or shopping tools such as pos machines.

Instead of the term cybercrime, concepts such as computer crime, internet crime, crimes committed in the electronic environment are also used. The transfer of information using electronic and technological tools can be described as *informatics*, and the crimes committed in this process can be described as *IT crimes (cyber crimes)*. Intervention in the information system; sometimes by having physical access to the system, sometimes by connecting remotely over the internet.

In addition to the fact that the 21st century is characterized as the "Information Age", the restriction of information exchange to milliseconds stands out as the only way for human beings to survive, as well as being insatiable with information. In this context, information technologies have grown to astonishing dimensions, covering the whole world like a spider web, permeating every aspect of our lives, and spreading over a wide concept without stopping. Now computers have an important role in human life and there is almost no work done without computers. However, to say that information technology has reached the end will cause a mistake in the sentence "everything that can be invented has been invented", allegedly said in 1899 by Charles H. Duell, Head

of the US Patent Office. Nowadays, people almost addictively transfer their lives to a cyber environment down to the last detail. Therefore, it is inevitable that all transactions to be made in the future will be done by computer. While this situation makes life easier by building the bridge between the world of information and the world of technology, it also causes the violation of human rights in the concept of informatics. Throughout the historical development, the changes that have occurred in the IT sector with high economic returns have brought problems. IT crime has forced the legislators to make new legal arrangements in order to protect users against malicious people and perhaps has revealed the necessity of creating a new branch of law.

While abacuses were used for counting before Christ, after the calculators produced in the 1800s, the world's first digital computer ENIAC, which weighs 30 tons, consists of 18000 vacuum tubes and is the ancestor of today's computers, was developed in II. With the development of the US army during World War II, the progress of information technologies began. The first commercially available computer, UNIVAC, was launched in 1952, and after the 1960s, electron tubes were replaced by first transistors and then integrated circuits that could be described as a combination of hundreds of transistors. After the Soviet Union sent the Sputnik satellite into space in 1957, the USA decided to manage the war systems placed in various parts of the world with a computer network in case of a war or confusion. The model created as a result of this was developed by US engineers in the 1970s and the structure known as the computer network today was created. Over time, this computer network was not limited to the army and academic units, but an information server (Internet or General network) containing millions of computers was formed. In the 1990s, computer networks have become widespread, with protocols called the Global Network (World Wide Web, WWW) developed at the CERN research center in Switzerland, applications such as e-mail, and inexpensive hardware solutions such as ethernet. In the 21st century, computers have come to fit in a wristwatch and run on a small battery. The limits of change, transformation and development in information technologies have reached a dimension equivalent to the unlimited imagination of human beings today. However, this development and transformation has brought with it the concept of cyber crimes.

Although there is no universally agreed definition of cybercrime, the most widely accepted definition was put forward at the Paris Meeting of the European Economic Community Experts Commission in May 1983, "any unlawful, immoral or unauthorized behavior in a system that automatically processes information or transfers data".

The world became acquainted with the phenomenon of cyber crimes at the end of the 1960s. With the formation of data banks in which personal data are processed in bulk, problems and threats to privacy started and firstly computer manipulation, sabotage and espionage crimes were seen. With the introduction of information networks in the 1970s, hacking acts such as hacking increased, and with the widespread use of personal computers in the 1980s, program hacking acts increased. In the same period, the use of ATMs in banking transactions brought about crimes related to debit cards. With the World Wide Web, it has started to be used in many legal and illegal transactions at an unimaginable speed, and many information, especially commercial and personal information, have become a target open to attack outside the borders of the country.

IT crimes have been classified differently in different sources according to criteria such as the purpose or tool of the computer, the violation of property rights, connection with information systems, computer use and the perpetrator of the crime. In the US doctrine, where cybercrime was first encountered, crimes were examined under 12 headings. These are;
1. Thefts against data or services
2. Thefts against property
3. Entry Violations
4. Data fraud
5. Errors caused by persons (Violations resulting from human errors)
6. Extortion
7. Violations against secrecy
8. Sabotages
9. Monetary thefts
10. Frauds committed in cases
11. Theft of ATM cards
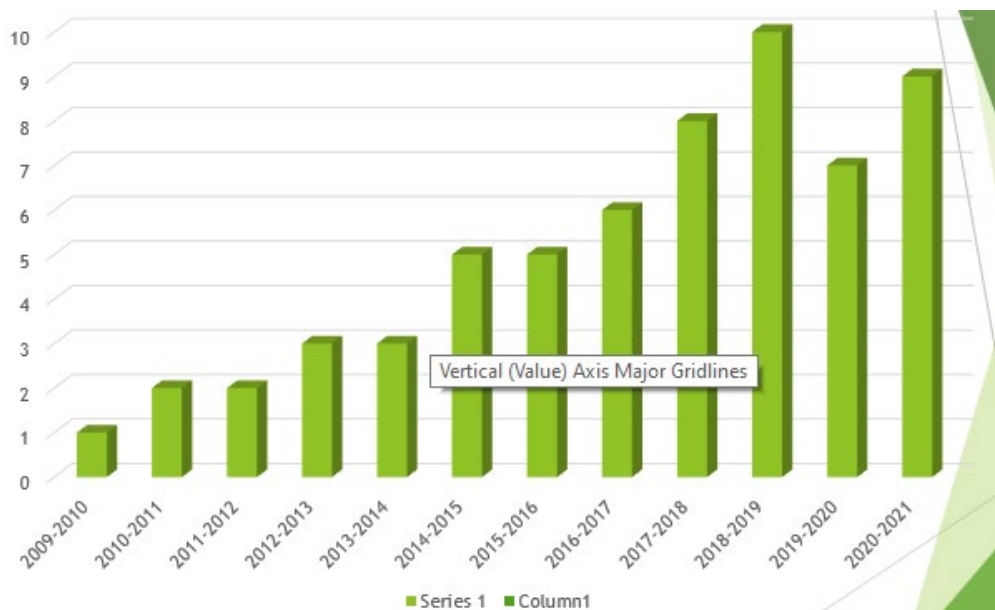12. Actions regarding the passwords of magnetic cards

FINDINGS
In order to reveal the IT Crime Rates in Schools, the IT crime distribution of Polatpaşa High School in the TRNC has been examined. According to the data obtained from Polatpaşa High School in TRNC, the number of

crimes related to informatics in the 2009-2021 academic years and the nature of the crimes are as shown in Table 1.

Academic Years	Number of Crimes	The Nature of the Crime
2009-2010	1	• To come to the exam hall with the mobile phone switched on.
2010-2011	2	• Using mobile phones in school
2011-2012	2	• Bringing the phone to the school, not following the school rules.
2012-2013	3	• Using a mobile phone at school • Taking photos of friends without permission.
2013-2014	3	• Bringing a phone to school without permission. • Attempting to cheat with a mobile phone.
2014-2015	5	• Bringing a phone to school without permission. • Sending a Facebook message to the teacher in the computer class.
2015-2016	5	• Bringing a phone to school without permission.
2016-2017	6	• Bringing a phone to school without permission. • Tampering with the mobile phone during the lesson. • Writing bad words about some girlfriends on social media.
2017-2018	8	• Bringing a phone to school without permission. • Entering the exam hall with the mobile phone switched on, attempting to cheat (not complying with the exam rules.). • Tampering with the mobile phone during the lesson.
2018-2019	10	• Bringing a phone to school without permission. • Watching inappropriate movies on a cell phone in the classroom. • Taking a photo of the female teacher with her back turned during the lesson.
2019-2020	7	• Shooting and posting the teacher without permission from a mobile phone. • Sending abusive messages on a mobile phone.
2020-2021	9	• Cheating with a mobile phone. • Cheating by plugging a wireless headset into a mobile phone.

Table 1. Distribution of number of crime and nature of crime in Polatpaşa high school between 2009-2021

Table 2. Graph about cybercrime by years in PPL

As can be seen in Table 1 and Table 2, cyber crimes in schools are increasing day by day. Despite the fact that schools are not open throughout the entire academic year due to the Covid 19 Pandemis, which has started all over the world since March 2019, the number of crimes has not decreased.

As it can be seen in Table 1, since there are no information-related articles in the "Disciplinary Regulations", there are gaps regarding these crimes. This creates a situation in favor of students who commit crimes. Again, as a result of the data obtained from Table 1, it was understood that students are prohibited from bringing mobile phones to school. The school administration held several meetings with the teachers on this issue. Meeting topic: "Should the mobile phone be banned or not?" As a result of the meeting, a full consensus could not be achieved. However, most of the teachers expressed an opinion that the use of mobile phones should be banned at school. Teachers stated that they complained about the use of mobile phones at school. Teachers expressed that they were worried about the crimes committed by mobile phones as well as negatively affecting the motivation of the students towards their school.   The other view is: "There is nothing we can solve by banning." he said. It also has a social dimension. It has been stated that there are parents who want to be informed about their children. It has been stated that it would be wrong to prevent this in the age of communication.

The Ministry of National Education should give an opinion on the inclusion of crimes committed by mobile phones in the "Disciplinary Regulation". It has been a common idea to start studies on the need to take action for mobile phone addiction, which has become a fearful dream of families and teachers and has reached serious dimensions in school-age children.

CONCLUSION AND RECOMMENDATIONS
In information technologies, it is useful as well as criminal activity.
There is an undeniable development and change that brings together the elements that can Today, informatics has become a concept that is associated with crime as well as being a technological revolution. When evaluated within this framework;
- It has become inevitable that cybercrimes should be handled comprehensively by lawmakers.
- New regulations to be created in the field of informatics should be regulated and universalized on the basis of the principles of sustainability in a way that protects the rights and freedoms of people and societies.
- It is imperative that new approaches and preventive, precautionary and protective practices against cybercrime are regulated by lawmakers.

With the advancement of technology every day, different types of crime emerge. In this context, the crime that is most open to change and development is cyber crimes. In the globalizing world, a new technological development is spreading all over the world. As a result, new cyber crimes are emerging in our country depending on the developing technology.

There are no laws and regulations regarding these crimes in schools in our country yet . Therefore, the existing "Disciplinary Regulations" should be renewed.

The by-law named as "Rules and Disciplinary Statute to be followed in and out of Secondary Schools and Secondary Education Institutions" was last drafted in 1989 and no additions were made afterwards. As a result of the needs emerging today, provisions related to informatics should be added to the Disciplinary Regulation.

It is obligatory to add the following items to the Rules and Discipline Regulations to be followed in and out of Secondary Schools and Secondary Education Institutions:
- It is forbidden to record or broadcast audio or video without permission in violation of personal rights.
- It is forbidden to prevent or disrupt the operation of an information system. This person is deemed to have committed a crime.
- It is forbidden to corrupt, destroy, change or render inaccessible data in an information system, to place data in the system, to send existing data to another place.
- It is forbidden to change, delete, render inaccessible or add new data to information data in a way that deceives others and for the purpose of using it as original information data by unlawfully operating on it, without seeking that this data is directly readable and understandable.
- It is forbidden to create informatics data in a way that deceives others, for the purpose of creating fake data with the appearance of original informatics data, without unlawfully taking action on it, without seeking that these data are directly readable and understandable.

Penalties that can be applied for these crimes according to the nature of the crime:
- Reprimand
- Written warning
- Short-term suspension from school
- Dismissal from the school

- Suspension from school with a school certificate
- Exclusion from formal education

REFERENCES

Akar, N. (2006). *Ortaöğretim Kurumlarında Karşılaşılan Disiplin Sorunları ve Eğitim Yöneticilerinin Çözüm Yaklaşımları (Denizli Örneği).* Unpublished Master's Thesis, Pamukkale University, Institute of Social Sciences, Denizli.

Aydın, E.(1984). *Bilişim Genel Sistemleri ve Sibernetik Terimleri Sözlüğü.* 256. İstanbul: Mistaş-Beytur A.Ş.

Başar, H. (2007). *Sınıf Yönetimi.* Ankara: Anı Publications.

Başaran, E. (2006). *Türk Eğitim Sistemi ve Okul Yönetimi.* Ankara: Ekinoks Publications.

Çelik, C. B. (2007). *Orta Dereceli Okul Öğrencilerinin Disipline Aykırı Davranışlarda Bulunma Nedenlerinin Araştırılması.* Unpublished Master Thesis, Yeditepe University, Institute of Social Sciences, Istanbul.

Çelik, K. (2008). Disiplin Oluşturma ve Kural Geliştirme, Kıran, H. (Ed.) *Etkili Sınıf Yönetimi*, (237-268), Ankara: Anı Publication.

Erkesici, E. (2005). *Meslek Liselerinde Öğrencilerin Disipline Aykırı Davranışlarda Bulunma Nedenleri(Ankara İli Örneği).* Unpublished Master Thesis, Gazi University, Institute of Educational Sciences, Ankara.

KKTC Bilişim Suçlari Yasasi, https://www.bthk.org/Documents/yasa-duzenleme/bilisimtasari.pdf Erişim tarihi: 15.06.2021

Özkök , A. (2005). Disiplinler arası Yaklaşıma Dayalı Yaratıcı Problem Çözme. Öğretim Programının Yaratıcı Problem Çözme Becerisine Etkisi *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi.* 28

Sarpkaya, P. (2005). Resmi Liselerde Disiplin Sorunları Ve İlgili Grupların (Öğretmen, Öğrenci, Yönetici, Veli) Yaklaşımları: Aydın Merkez İlçe Örneği. Unpublished Doctoral Thesis, Dokuz Eylul University, Institute of Educational Sciences, Izmir.

Şengul, T. (2005). Geleneksel ve çağdaş eğitim anlayişinda ilgi ve disiplin. Milli Eğitim Üç Aylık Eğitim ve Sosyal Bilimler Dergisi, Spring, 166.