DOI: https://doi.org/10.36719/2706-6185/33/91-95

Arzu Shukurova
Baku State University
master student
arzushukur@yahoo.com

DEFINITION OF INFORMATION TECHNOLOGIES AND TYPES OF CRIMES COMMITTED THROUGH THEM

Abstract

The field of information technologies, as well as the related legal fields arising from the need to regulate this field - information law, information technology law, internet law, cyber law are not only a new field, but also areas that need extensive research.

Since it is a new field, there is a need to analyze and improve the national legislation related to the field. At the same time, the difficulty of finding the equivalent of the terms and concepts used in this field in the Azerbaijani language causes a small number of literature and sources in our native language. In order for crimes committed through information technologies to be detected, correctly evaluated, described and explained, as well as for the perpetrators of these crimes to be legally and fairly punished, it is extremely important that these types of crimes are researched, investigated and reflected in relevant legislative acts. Taking these into account, in addition to the understanding of information technologies, the article shows the types of crimes committed through these technologies, and also gives a brief explanation about each of them.

Keywords: *information technologies, IT law, cybercrimes, data privacy, identity theft, information, fraud*

Arzu Şükürova
Bakı Dövlət Universiteti
magistrant
arzushukur@yahoo.com

İnformasiya texnologiyalarının anlayışı və onlar vasitəsilə törədilən cinayətlərin növləri

Xülasə

İnformasiya texnologiyaları sahəsi, habelə bu sahənin tənzimlənməsi zərurətindən meydana gələn əlaqəli hüquq sahələri – informasiya hüququ, informasiya texnologiyaları hüququ, internet hüququ, kiber hüquq yeni bir sahə olmaqla yanaşı, geniş tədqiq olunmağa da ehtiyacı olan sahələrdir.

Yeni sahə olduğundan sahə ilə əlaqəli milli qanunvericiliyin də təhlil edilməsinə və bu mövzuda təkmilləşdirilməsinə ehtiyac vardır. Eyni zamanda, bu sahədə istifadə olunan termin və anlayışların Azərbaycan dilində qarşılığının tapılmasının çətinliyi ana dilimizdə olan ədəbiyyat və mənbələrin də sayının azlığına səbəb olur. İnformasiya texnologiyaları vasitəsilə törədilən cinayətlərin aşkar oluna bilməsi, doğru dəyərləndirilə, tövsif və izah oluna bilməsi, eləcə də bu cinayətləri törədənlərin hüquqi cəhətdən ədalətli cəzalandırıla bilməsi üçün bu növ cinayətlərin tədqiqi, araşdırılması və müvafiq qanunvericilik aktlarında öz əksini tapması olduqca vacibdir. Bunlar nəzərə alınaraq, məqalədə informasiya texnologiyalarının anlayışı ilə yanaşı, bu texnologiyalar vasitəsilə törədilən cinayətlərin növləri göstərilmiş, həmçinin hər biri barədə qısa izah verilmişdir.

Açar sözlər: *informasiya texnologiyaları, İT hüququ, kiber cinayətlər, məlumat gizliliyi, şəxsiyyət oğurluğu, informasiya, saxtakarlıq*

Introduction

In the Republic of Azerbaijan, the formation of information resources based on the collection, processing, storage, search, and distribution of information, information systems, technologies, the creation and use of their security means, and relations arising in connection with information protection are regulated by the Law "On Information, Informatization and Information Protection". According to Article 2 of this Law, information technology means the system of methods and tools used during information processes, including the application of computing and communication techniques (1; Aliyev, Rzayeva, İbrahimova, 2019).

Computers are considered the main technical means of information technologies. From a technological point of view, the function of computer technologies as an object of transmission, storage, and processing is to ensure the efficiency of using information resources, to produce information to increase the reliability and efficiency of processes (Aliyev, Rzayeva, İbrahimova, 2019: 244). According to the aforementioned Law, information is facts, opinions, news or other information created or obtained as a result of any activity, regardless of the date of creation, presentation form and classification (1; Aliyev, Rzayeva, İbrahimova, 2019).

Information technologies have passed a path of about 4 centuries to the current level of development. In the 60s of the 20th century, the first modern information systems began to be created and improved, and since the end of the 20th century, the development of information technologies has intensified due to the popularization of the Internet, the development of Scientific and Technical Progress, the creation of new technical tools for information processing - ultramodern programs and systems, especially the application of computers in the information environment and the use of telecommunication tools have brought the development of information technology to a new stage (Aliyev, Rzayeva, İbrahimova, 2019: 244).

With the development of information technologies, new concepts have emerged, and the emergence of such new concepts and relationships has created conditions for the creation of new legal fields.

Thus, in the countries with the Anglo-American legal system, several legal fields related to information communication technologies have been formed. The first of these is considered the information technology law (Information Technology Law - IT Law) and covers the legal aspects of the use of information communication technologies in society. Such legal issues include access to and dissemination of digital information, software, electronic signatures, and security issues. A second area of law is internet law (cyber law) and includes legal aspects related to the Internet (Aliyev, Rzayeva, İbrahimova, 2019: 13).

Information technology law, often known as Internet law or cyber law, is a branch of the legal system concerned with legal informatics that regulates the digital exchange of information, e-commerce, software, and data security. It’s linked to legal informatics and electronic components like computers, software, and hardware. It covers a wide range of themes, including access to and use of the internet and freedom of speech and online privacy (3). Cybercrime law includes laws related to computer crimes, internet crimes, information crimes, communications crimes, and technology crimes. While the internet and the digital economy represent a significant opportunity, they’re also an enabler for criminal activity. Cybercrime laws are laws that create the offences and penalties for cybercrimes (4).

Cybercrime describes crimes directed at computers, data or information communications technologies and crimes committed by people using computers or ICT. Cybercrime is a global problem, which requires a coordinated international response (4).

Cyber crime can be categorized mainly in two ways:

- Using the Computer as a Target: using a computer to attack other computers. e.g. Hacking, Virus/Worm attacks, DOS attack etc.
- Using the computer as a weapon: using a computer to commit real world crimes. e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc (7).

New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy. All those activities existed before the "cyber" prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behaviour alongside some novel illegal activities (8).

Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity (8).

An important aspect of cybercrime is its nonlocal character: actions can occur in jurisdictions separated by vast distances. This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation. For example, if a person accesses child pornography located on a computer in a country that does not ban child pornography, is that individual committing a crime in a nation where such materials are illegal? Where exactly does cybercrime take place? Cyberspace is simply a richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation. As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself. However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals leave clues as to their identity and location, despite their best efforts to cover their tracks. In order to follow such clues across national boundaries, though, international cybercrime treaties must be ratified (8).

Here are some of the most common types of identity theft and fraud:

Financial identity theft is the most common form of identity theft, and it can be a lot more trouble than just replacing a credit card. In this type of theft, bank account numbers, credit cards, or personally-identifying information can be used to wipe out your accounts, take out loans, or get new credit cards. You could be held financially responsible for purchases, loans, rentals or other transactions made in your name. Unpaid bills could damage your credit rating, making it impossible for you to get a home, auto, or college loan or to rent housing (9). **Medical identity** theft happens when criminals sell your personal medical information or make fraudulent claims against your health policy. If your medical identity is stolen, you could be charged for medical services received by someone impersonating you. You could be denied medical services if those bills exceed the limits of your medical coverage. And someone else's information could end up in your medical file, putting you at risk for life-threatening misdiagnosis or mistreatment (9).

Viruses and malicious code are programs which are designed to run on home and office computers. They have various destructive intents which may permanently or temporarily disable a computer. Some programs such as worms are self replicating and can therefore infect large numbers of systems in a very short space of time (4). **Unauthorized access** to electronic data or to a computer system can result in the misuse of that data. For example, there have been several instances where the credit card databases of various companies have been fraudulently accessed and the credit card details of all of the customers of the company posted online (4).

The term 'internet fraud' refers to any type of fraud scheme that uses email, web sites, chat rooms or message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme. Internet fraud may include spam, scams, spyware, identity theft, phishing or internet banking fraud (10).

Spam is a generic term used to describe electronic 'junk mail' or unwanted messages sent to your email account or mobile phone (10). Spam can carry advertising that is annoying but benign; however, it can also be an initial contact point for cybercriminals - like the operators of a fraudulent scheme who use emails to solicit money from prospective victims, as in advance fee frauds, or to commit identity theft by deceiving recipients into sharing their personal, banking and financial information. It can also be used to deliver malware like computer viruses, worms and ransomware, or to distribute child exploitation material (Lloyd, 2011).

Spyware is generally considered to be software that is secretly installed on a computer and takes things from it without the permission or knowledge of the user. Spyware may take personal information, business information, bandwidth or processing capacity and secretly gives it to someone else. It is recognised as a growing problem (10).

Phishing is a technique used to gain personal information for the purpose of identity theft. Phishing involves using a form of spam to fraudulently gain access to people's online banking details. As well as targeting online banking customers, phishing emails may target online auction sites or other online payment facilities. Typically, a phishing email will ask an online banking customer to follow a link in order to update personal bank account details. If the link is followed the victim downloads a program which captures his or her banking login details and sends them to a third party (10).

Internet banking fraud is a fraud or theft committed using online technology to illegally remove money from a bank account and/or transfer money to an account in a different bank. Internet banking fraud is a form of identity theft and is usually made possible through techniques such as phishing (10). By the early 1980s, communication between geographically separate computer systems was possible, and with it the possibility of external access to computer systems. Although the terms 'hacking' and 'hacker' have a lengthy and, indeed, respectable pedigree in computer technology, they have now become largely synonymous with the act of obtaining unauthorised access to a computer system and, more specifically, obtaining this access by means of a telecommunications connection from another computer (Lloyd, 2011: 215). **Hacking** is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system, Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cybercrimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks (12).

Conclusion

From what has been written above, we can conclude that each of these listed crimes is committed in cyberspace and with the help of technological means. In order to be able to detect these types of crimes, first of all, it is necessary to be familiar with the concept of information technology.

This responsibility falls primarily on the police, investigators, prosecutors, judges, as well as persons working in all law enforcement agencies. For this reason police, prosecutors and judges need to understand these crimes and must have the appropriate tools to enable them to investigate and prosecute offenders as well as protect victims. They must also be able to process and prosecute cases.

In addition, the classification and types of cybercrimes should be studied, their nature should be known, and then incorporated into local legislation. As well as, serious educational measures about the methods and means of committing this type of crimes should be taken among the population, especially among children and teenagers. Countries should also cooperate among themselves to prevent and detect such crimes. Interstate relations in this area should be expanded, and the number

of bilateral and multilateral agreements should increase. Besides this, international organizations should be interested in establishing such cooperation and should encourage countries to this cooperation.

Reference

1. The Law on "Information, Informatization and Information Protection" of the Republic of Azerbaijan.
2. Aliyev, A., Rzayeva, G., İbrahimova, A. (2019). Behruz Meherremov, Shahin Memmedrzali, İnformation law. Book.
3. https://unacademy.com/content/upsc/study-material/law/information-technology-law/
4. https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world
5. https://www.researchgate.net/publication/274652160_Cyber_Crime_its_Categories
6. https://www.britannica.com/topic/cybercrime#ref235699
7. https://www.idx.us/knowledge-center/a-savvy-consumers-guide-to-privacy-identity-theft
8. United Nations Economic Commission for Europe - Information and Communication Technology Policy and Legal Issues for Central Asia - Guide for ICT Policymakers, 2007.
9. https://www.police.act.gov.au/sites/default/files/PDF/bizsafe-internet-fraud-factsheet.pdf
10. https://www.researchgate.net/publication/306035643_An_Analysis_of_the_Nature_of_Spam_as_Cybercrime
11. Lloyd, I.J. (2011). Professor, Information Technology Law, Book, Sixth Edition.
12. https://www.researchgate.net/publication/333632435_Ethical_Hacking_and_Knowledge_about_Hacking

Received: 26.12.2023 Accepted: 10.03.2024