УДК 343.7

А.М. Соловйова
кандидат юридичних наук,
докторант Класичного Приватного університету

НЕПРАВОМІРНИЙ ДОСТУП ДО ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ ЯК ЗЛОЧИН ПРОТИ ВЛАСНОСТІ ЗА ЗАКОНОДАВСТВОМ ЗАРУБІЖНИХ КРАЇН

Soloviova Alina
Candidate of Juridical Sciences
Doctoral student
of Classical Private University

LEGAL ACCESS TO TELECOMMUNICATIONS SERVICES AS A CRIME AGAINST PROPERTY UNDER THE LAWS OF FOREIGN COUNTRIES

Since Wheatstone and Cooke first patented their system of communication by the means of electromagnetic impulses carried over wires in 1837, crimes have been committed either through the misuse of telecommunications equipment, or against telecommunications equipment.

Every technological development has provided a new opportunity for criminality which has often been utilized. Unfortunately, as we move into the twenty-first century where broadband telecommunications services such as interactive video telephony will become widely available; the opportunities for criminality will be enhanced [1].

Telecommunications technology has begun to provide criminal opportunities of unprecedented scope and dimension. The revolution in information technology which we are currently experiencing is perhaps the most significant development of our time. Recent and anticipated changes in telecommunications technology in light of the connectivity of communications and computing are truly breathtaking, and have already had significant impacts on many aspects of life.

Banking, stock exchanges, air traffic control, telephones, electric power, and a wide range of institutions of health, welfare, and education are largely dependent on information technology and telecommunications for their operation [2].

Computer-related crime, like crime in general, may be explained by the conjunction of three factors, motivation, opportunity and the absence of capable guardianship. Motivations will vary depending on the nature of the crime in question, but may include, greed, lust, revenge, challenge or adventure.

Opportunities are expanding dramatically with the rapid proliferation and penetration of digital technology. Significant challenges are posed by the transnational nature of much computer crime.

The most appropriate strategies for the control of computer-related crime entail a mixture of law enforcement, technological and market-based solutions. Significant challenges arise from the transnational nature of much computer crime, and from the need for the law to keep abreast of developments in technology and their criminal exploitation [3].

Illegal access to telecommunications services is becoming more common in today's information society.

Therefore, in recent years some national legislators have been providing illegal access to telecommunications services as an independent property crime (Albania, Azerbaijan, Iran, Spain, China, Colombia, Lithuania, Netherlands, Poland, USA).

The "phone phreakers" of three decades ago set a precedent for what has become a major criminal industry. By gaining access to an organisation's telephone switchboard (PBX) individuals or criminal organisations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties (Gold 1999).

Offenders may gain access to the switchboard by impersonating a technician, by fraudulently obtaining an employee's access code, or by using software available on the internet. Some sophisticated offenders loop between PBX systems to evade detection. Additional forms of service theft include capturing "calling card" details and on-selling calls charged to the calling card account, and counterfeiting or illicit reprogramming of stored value telephone cards [3].

Ever since the original "phreakers" of a quarter-century ago attacked telecommunications systems out of curiosity, telecommunications services have been vulnerable to theft. From those whose motives were confined to simple mischief-making, to those who have made theft of services a way of life and a major criminal industry, those who steal services pose a significant challenge to telecommunications carriers, service providers, and to the general public, who often bear the financial burden of fraud. The market for stolen telecommunications services is large indeed.

There are those who simply seek to avoid or to obtain a discount on the cost of a telephone call. There are others, such as illegal immigrants, who are unable to acquire legitimate telecommunications services without disclosing their identity and their status. There are others still who appropriate telecommunications services to conduct other illicit business with less risk of detection. Across the world, immense sums of money are lost by the victims of such illegality. Substantial sums are also incurred in preventing, detecting and prosecuting offences [2].

Scientists from USA highlighted three major categories of telecom fraud. These categories are: • Traffic Pumping Schemes – These schemes use "access stimulation" techniques to boost traffic to a high cost destination, which then shares the revenue with the fraudster. • Schemes to Defraud Telecom Service Providers - These schemes are the most complicated, and exploit telecom service

providers using SIP trunking, regulatory loopholes, and more. • Schemes Conducted Over the Telephone - Also known as "Phone Fraud," this category covers all types of general fraud that are perpetrated over the telephone [4].

Eugenio Rosas and Cesar Analide also termed common fraud types. They stress that it is not possible to enumerate completely and exhaustively all the existing fraud types. Due to the constant evolution of technology existing fraud types are adapted and new fraud types are developed all the time. However, there is a set of the major fraud causes that are the ones of most concern to the telecommunications operators at the time. These are: – Subscription fraud - one of the most common fraud types along with the SIM cloning.

The fraudster obtains the service from the operator with no intention to pay for it, using a false identity. The damage this fraud type causes depends on the intention of the fraudster: using the service for personal use until he is detected; on a more sophisticated level, the fraudster can use the service in order to profit from the use of it. – Bypass fraud - deprives the terminating operator of interconnect termination fees for incoming international calls. This is usually done using VoIP technology to bypass international calls. – SIM cloning - a fraudster clones an existing normal SIM card. The software to clone SIM cards is available on the internet, so if a fraudster has physical access to a SIM card all he needs to clone it is a PC and a card reader.

This is considered the most common fraud cause of all. – Internal fraud – implies action of internal staff of the operators. Typically, operator employees with knowledge and access to the information systems, handle information in order to benefit a third party, for instance: giving free minutes, changing account settings[5].

Scientists from Israel Saharon Rosset, Uzi Murad, Einat Neumann, Yizhak Idan, Gadi Pinkas noted that the telecommunications industry suffers major losses due to fraud. The various types of fraud may be classified into two categories: Subscription fraud – fraudsters obtain an account without intention to pay the bill. In such cases, abnormal usage occurs throughout the active period of the account.

The account is usually used for call selling or intensive self-usage. Cases of bad debt, where customers who do not necessarily have fraudulent intentions never pay a single bill, also fall into this category. These cases, while not always considered as "fraud", are also interesting and should be identified. Superimposedfraud - fraudsters "take over" a legitimate account. In such cases, the abnormal usage is superimposed upon the normal usage of the legitimate customers. Examples of such cases include cellular cloning, calling card theft and cellular handset theft [6].

In France, the jurisprudence has recognized qualification as unjustified kidnapping illegal use of telephone, computer information systems, as well as illegal adoption of encoded TV programs. After such judgments in the former Criminal Code of France in 1987, it was amended.

After the adoption of the current Criminal Code provisions on these crimes were transferred to the law on freedom of communication (1986).

Theft of services on the Swiss Code is in the form of non-payment on the account in the hotel or restaurant in the form of the acquisition of services by deception. According to art. 149 of the Criminal Code of Swiss, the one who lived

in a hotel, ordering food and drink or get other services in the institutions and does not make their payment to the owner shall be punished by imprisonment or a fine.

The Canadian Criminal Code (R.S.C. 1985, c. C-46) establishes a number of specific offences dealing with telecommunications, notably theft of a telecommunication service (s. 326) and possession of device to obtain telecommunication facility or service (s.327).

Other criminal provisions dealing with the unauthorized use of a computer and invasion of privacy are beyond the scope of the present article. For the purposes of these two sections, «telecommunication» is defined as any transmission, emission or reception of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio, visual, or other electromagnetic system, which encompasses in exhaustive manner any form of communication at a distance (s. 326(2)) [7].

In the Netherlands, as in many other jurisdictions, the national criminal law comprises inchoate crimes. Basically, general doctrine recognizes three separate forms of these: attempt, preparation and conspiracy.

Conspiracy is criminalized only for offences against the state and terrorist attacks, where there is a widespread hesitation to criminalize conspiracy as under the common law. Criminal liability is preferably connected to an overt act, to be specified in the statutory description of the crime.

Therefore a broad general criminalization of conspiracy is rejected as lacking the necessary specification. At het moment it has no statutory basis. In this chapter we will deal with some general observations on attempt and preparation as incomplete forms of causing damage to the interests protected by the law on cyber crime [8].

Thus, telecommunications fraud is a problem that affects operators all around the world. Scientists from around the world emit several types of these crimes. To date, Ukrainian Criminal Code has not criminalized the offense. But world practice shows that telecommunications fraud continues to be a big problem in the industry today. With fraud continuing to be a big problem, fraud management has evolved from a defensive and reactive strategy focused on prevention to a more proactive, revenue generating and innovative approach.

REFERENCES:

1. *Smith Russell*. Stealing Telecommunications Services / Russell G. Smith // Electronic resource: http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi054.pdf

2. *Grabosky P.N.* Crime and Telecommunications / P.N. Grabosky, Russell G. Smith, Paul Wright // Electronic resource: http://aic.gov.au/media_library/publications/tandi_pdf/tandi059.pdf

3. *Grabosky Peter*. Computer crime in a world without borders /Peter Grabosky // Electronic resource: http://www.crime-research.org/library/Peter.htm

4. Telecom fraud call scenarios // Electronic resource: http://transnexus.com/wp-content/uploads/TFS.pdf

5. *Rosas Eugenio*. Telecommunications Fraud: Problem Analysis – an Agent-based KDD Perspective / Eugenio Rosas, Cesar Analide // Electronic resource: http://epia2009.web.ua.pt/onlineEdition/402.pdf

6. Rosset Saharon. Discovery of Fraud Rules for Telecommunications - Challenges and Solutions/ Saharon Rosset, Uzi Murad, Einat Neumann, Yizhak Idan, Gadi Pinkas // Electronic resource:http://www.tau.ac.il/~saharon/papers/fraud.pdf

7. *Gravelle Louis-Pierre*. Canadian criminal provisions dealing with telecommunications/Louis-Pierre Gravelle // Electronic resource: http://www.robic.ca/admin/pdf/578/222-03LPG.pdf

8. *Stamhuis Evert*. Criminal law on cyber crime in the Netherlands / Evert F. Stamhuis // Electronic resource: http://www.penal.org/sites/default/files/files/RV-11.pdf

Soloviova A. Legal access to telecommunications services as a crime against property under the laws of foreign countries

The article investigates the illegal access to telecommunications services as one of the crimes against property. The author systematized different approaches to the definition and types of illegal access to telecommunication services. In the article analyzed the international practice of recognizing the illegal access to telecommunications services as a crime against property.

Keywords: *crime, theft, property damage, telecommunication services, crimes against property.*

Соловйова А.М. Неправомірний доступ до телекомунікаційних послуг як злочин проти власності за законодавством зарубіжних країн

У статті досліджується неправомірний доступ до телекомунікаційних послуг як один із злочинів проти власності. Автором систематизовано різні підходи до визначення поняття та видів неправомірного доступу до телекомунікаційних послуг. Аналізується міжнародна практика визнання неправомірного доступу до телекомунікаційних послуг як злочину проти власності.

Ключові слова: *злочин, крадіжка, майнова шкода, телекомунікаційні послуги, злочини проти власності.*

Соловьева А.Н. Неправомерный доступ к телекоммуникационным услугам как преступление против собственности по законодательству зарубежных стран

В статье исследуется неправомерный доступ к телекоммуникационным услугам как один из преступлений против собственности. Автором систематизированы различные подходы к определению понятия и видов неправомерного доступа к телекоммуникационным услугам. Анализируется международная практика признания неправомерного доступа к телекоммуникационным услугам как преступления против собственности.

Ключевые слова: *преступление, кража, имущественный вред, телекоммуникационные услуги, преступления против собственности.*

Стаття надійшла до редакції 07.12.2015.