СЕКЦІЯ 2. ДИСКУРС ЮРИДИЧНИХ НАУК

Elsie Appiah
Research supervisor: Tetyana Drakokhrust
Candidate of Law Sciences, Associate Professor
Language tutor: Nataliia Sobetska,
Candidate of Philological Sciences, Associate Professor
Ternopil National Economic University

CYBER CRIME IN NOWADAYS REALITY

The development in information technology and electronic media especially from 1980's onwards have given rise to a new variety of computer related crimes which are commonly called "cybercrimes". The widespread growth of these crimes has become a matter of global concern and a challenge for the law enforcement agencies in the new millennium. Because of the peculiar nature of these crimes, they can be committed anonymously and far away from the victim without being physically present there. Further cyber criminals have a major advantage; they can use computer technology to inflict damage without risk of being caught. These crimes cover a wide range of illegal computer-related activities such as theft of communication services, industrial espionage, dissemination of pornographic and sexy offensive material in cyber-space, electronic money laundering and tax evasion, electronic vandalism, terrorism and extortion, tele-marketing frauds, illegal interception of tele-communication etc.

Some authorities feel that the term 'cyber-crime' is a misnomer as this term is nowhere defined in any statute or Act enacted by the Parliament. In a sense, it is not radically different from the concept of conventional crime insofar as both include conduct whether act or omission, which causes breach of law and therefore, it is punishable by the state. A cyber-crime may be defined as any criminal activity that uses a computer either as an instrumentality, target or means of perpetrating further crime. In other words, cybercrime is an unlawful act wherein the computer is either a tool or a target or both. The distinction between cybercrime and conventional crime lies in the involvement of the medium in cases of cybercrime.

That is, there should be involvement, at any stage, of the virtual cyber space medium in case of a cybercrime. The types of cyber-crimes include pornography, cyber fraud, defamation, cyber stalking, harassment, IPR theft, data hostage, money laundering, phishing, e-mail bombing, cyber war, illegal EFT. Cyber-crime is different and more heinous than conventional crime as in cyber-crime; the crime is committed in an electronic medium and here means read is not a requirement but is rather a general rule under the penal provisions of the Information Technology Act. The Indian Parliament considered it necessary to give effect to the resolution by which U.N. General Assembly adopted Model Law on Electronic Commerce adopted by the United Nations Commission on Trade Law. As a consequence of which the Information Technology Act, 2000 was passed. This Act was a welcome step at a time when there was no legislation on this field.

The Act has however during its application proved to be inadequate and there are certain loopholes in the Act. Cyber Crime in the Act is neither comprehensive nor exhaustive. The Information Technology Act has not dealt with cyber nuisance, cyber stalking, and cyber defamation and so on. Cases of spam, hacking, stalking and e-mail fraud are rampant although cyber-crimes cells have been set-up in major cities. The problem is that most cases remain unreported due to lack of awareness.

Capacity of human mind is unfathomable. It is not possible to eliminate cyber crime from the cyber space. However, it is quite possible to check them. The home user segment is the largest recipient of cyber-attacks as they are less likely to have established security measures in place and therefore it is necessary that people should be made aware of their rights and duties.

Users must try and save any electronic information trail on their computers, use of anti-virus software, firewalls, use of intrusion detection system etc. and further making the application of the laws more stringent to check crime. Cyber-crimes against person or individual include harassment via e-mail, stalking, defamation, unauthorized access to computer systems, indecent exposures; e-mail spoofing, fraud, cheating and pornography etc. Computer related crimes against property include computer vandalism, transmission of virus, denial of service at lack, unauthorized access over

computer system, intellectual property rights violations, Internet time-theft, sale of illegal articles etc.

Cyber-crimes against state or society may comprise possession of unauthorized information, cyber terrorism, distribution of pirated software, polluting youth through indecent exposure, trafficking financial scams, forgery, online gambling etc. Some of the cyber-crimes which are generally committed in the cyber space through computer systems are explained as follows,

In stalking, persistent messages are sent to unwilling recipients, thus causing them annoyance, worry and mental torture. Sending of unsolicited e-mails or spamming is an infringement of right of privacy. Online harassment and threats may take many forms. Cyber stalking usually occurs with women who are stalked by men, adolescents or adult pedophiles. A cyber stalker does not have to leave his home to harass his targets and has no fear of physical avenge since he cannot be physically touched in cyber space. A cyber stalker generally collects all the personal information about the victim such as name, age, family background, telephone or mobile numbers, workplace etc. He collects this information from the internet resources such as various profiles the victim may have filled-in while opening the chat or e-mail account.

The menace of cyber stalking has spread like wild-fire in India and many innocent women, girls and children are being targeted as its victim.

References:

1. "Cybercriminals Need Shopping Money in 2017, Too! - SentinelOne". sentinelone.com. 2016-12-28. Retrieved 2017-03-24.
2. Easttom C. (2010) Computer Crime Investigation and the Law
3. Gordon, Sarah (July 25, 2006). "On the definition and classification of cybercrime" (PDF). Retrieved January 14, 2018.