

Philippines: Proposed Cybercrime Prevention Act

Policy declaration

- to provide an environment conducive to the application of ICT to attain free, easy, and intelligible access to exchange and delivery of information
- to protect and safeguard the integrity of computer, computer and communications systems, networks, and database, and the confidentiality, integrity, and availability of information and data stored therein from all forms of misuse and abuse
- recognize the need for fast and reliable international cooperation

Chapter I - Definition of Terms

- Cybercrime – refers to any offense that can be committed by using a computer or communications system or network in a computer or communications system or network against a computer or communications system or network
- Service Provider – refers to the provider of telecommunications and online services or network access, or the operator of communications and network facilities, including entities offering the transmission, routing, or providing of connections for online communications, digital or otherwise, between or among point specified by a user, of electronic documents of the user's choosing; or any other entity that processes or stores information on behalf of such communication service or users of such service

Chapter II - Punishable Acts

- A. Computer Crime
 1. Illegal access
 2. Illegal interception
 3. Misuse of devices
 4. Unsolicited commercial transactions
- B. Computer Sabotage
 1. Data Interference
 2. System Interference
 3. Computer Fraud
 4. Computer Forgery
- C. Computer Facilitated Crime
 1. Offenses related to Cybersex
 2. Violations of the Revised Penal Code, Intellectual Property Code, Consumer Act and Relevant Laws

Chapter IV - Computer Emergency Response Council (CERC)

Chapter V - Enforcement and Implementation

Chapter VII - International Cooperation