[AS PASSED BY THE MAJLIS-E-SHOORA (PARLIAMENT)]

A

BILL

to make provisions for prevention of electronic crimes

WHEREAS it is expedient to prevent unauthorized acts with respect to information systems and provide for related offences as well as mechanisms for their investigation, prosecution, trial and international cooperation with respect thereof and for matters connected therewith or ancillary thereto:

It is hereby enacted as follows: -

CHAPTER I
PRELIMINARY

1. **Short title, extent, application and commencement**.- (1) This Act may be called the Prevention of Electronic Crimes Act, 2016.

(2) It extends to the whole of Pakistan.

(3) It shall apply to every citizen of Pakistan wherever he may be and also to every other person for the time being in Pakistan.

(4) It shall also apply to any act committed outside Pakistan by any person if the act constitutes an offence under this Act and affects a person, property, information system or data located in Pakistan.

(5) It shall come into force at once.

2. **Definitions**.- (1) In this Act, unless there is anything repugnant in the subject or context,

(a) "act" includes-

(i) a series of acts or omissions contrary to the provisions of this Act; or

(ii) causing an act to be done by a person either directly or through an automated information system or automated mechanism or self-executing, adaptive or autonomous device and whether having temporary or permanent impact;

(b) "access to data" means gaining control or ability to use, copy, modify or delete any data held in or generated by any device or information system;

(c) "access to information system" means gaining control or ability to use any part or whole of an information system whether or not through infringing any security measure;

(d) "Authority" means the Pakistan Telecommunication Authority established under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996);

(e) "authorization" means authorization by law or the person empowered to make such authorization under the law:

Provided that where an information system or data is available for open access by the general public, access to or transmission of such information system or data shall be deemed to be authorized for the purposes of this Act;

(f) "authorized officer" means an officer of the investigation agency authorized to perform any function on behalf of the investigation agency by or under this Act;

(g) "Code" means the Code of Criminal Procedure, 1898 (Act V of 1898);

(h) "content data" means any representation of fact, information or concept for processing in an information system including source code or a program suitable to cause an information system to perform a function;

(i) "Court" means the Court of competent jurisdiction designated under this Act;

(j) "critical infrastructure" means critical elements of infrastructure namely assets, facilities, systems, networks or processes the loss or compromise of which could result in:

(i) major detrimental impact on the availability, integrity or delivery of essential services – including those services, whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; or

(ii) significant impact on national security, national defense, or the functioning of the state".

Provided that the Government may designate any private or Government infrastructure in accordance with the objectives of sub-paragraphs (i) and (ii) above, as critical infrastructure as may be prescribed under this Act.

(k) "critical infrastructure information system or data" means an information system, program or data that supports or performs a function with respect to a critical infrastructure;

(l) "damage to an information system" means any unauthorized change in the ordinary working of an information system that impairs its performance, access, output or change in location whether temporary or permanent and with or without causing any change in the system;

(m) "data" includes content data and traffic data;

(n) "data damage" means alteration, deletion, deterioration, erasure, relocation, suppression of data or making data temporarily or permanently unavailable;

(o) "device" includes-

(i) physical device or article;

(ii) any electronic or virtual tool that is not in physical form;

(iii) a password, access code or similar data, in electronic or other form, by which the whole or any part of an information system is capable of being accessed; or

(iv) automated, self-executing, adaptive or autonomous devices, programs or information systems;

(p) "dishonest intention" means intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred or incitement to violence;

(q) "electronic" includes electrical, digital, magnetic, optical, biometric, electrochemical, electromechanical, wireless or electromagnetic technology;

(r) "identity information" means an information which may authenticate or identify an individual or an information system and enable access to any data or information system;

(s) "information" includes text, message, data, voice, sound, database, video, signals, software, computer programmes, any forms of intelligence as defined under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996) and codes including object code and source code;

(t) "information system" means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information;

(u) "integrity" means, in relation to an electronic document, electronic signature or advanced electronic signature, the electronic document, electronic signature or advanced electronic signature that has not been tampered with, altered or modified since a particular point in time;

(v) "interference with information system or data" means and includes an unauthorized act in relation to an information system or data that may disturb its normal working or form with or without causing any actual damage to such system or data;

(w) "investigation agency" means the law enforcement agency established by or designated under this Act;

(x) "minor" means, notwithstanding anything contained in any other law, any person who has not completed the age of eighteen years;

(y) "offence" means an offence punishable under this Act except when committed by a person under ten years of age or by a person above ten years of age and under fourteen years of age, who has not attained sufficient maturity of understanding to judge the nature and consequences of his conduct on that occasion;

(z) "rules" means rules made under this Act;

(za) "seize" with respect to an information system or data includes taking possession of such system or data or making and retaining a copy of the data;

(zb) "service provider" includes a person who-

(i) acts as a service provider in relation to sending, receiving, storing, processing or distribution of any electronic communication or the provision of other services in relation to electronic communication through an information system;

(ii) owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or

(iii) processes or stores data on behalf of such electronic communication service or users of such service;

(zc) "subscriber information" means any information held in any form by a service provider relating to a subscriber other than traffic data;

(zd) "traffic data" includes data relating to a communication indicating its origin, destination, route, time, size, duration or type of service;

(ze) "unauthorized access" means access to an information system or data which is not available for access by general public, without authorization or in violation of the terms and conditions of the authorization;

(zf) "unauthorized interception" shall mean in relation to an information system or data, any interception without authorization; and

(zg) "Unsolicited information" means the information which is sent for commercial and marketing purposes against explicit rejection of the recipient and does not include marketing authorized under the law.

(2) Unless the context provides otherwise, any other expression used in this Act or rules made thereunder but not defined in this Act, shall have the same meanings assigned to the expressions in the Pakistan Penal Code, 1860 (Act XLV of 1860), the Code of Criminal Procedure, 1898 (Act V of 1898) and the Qanoon-e-Shahadat Order, 1984 (P.O.No.X of 1984), as the case may be.

CHAPTER II
OFFENCES AND PUNISHMENTS

3. **Unauthorized access to information system or data.**- Whoever with dishonest intention gains unauthorized access to any information system or data shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both.

4. **Unauthorized copying or transmission of data.-** Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any data shall be punished with imprisonment for a term which may extend to six months, or with fine which may extend to one hundred thousand rupees or with both.