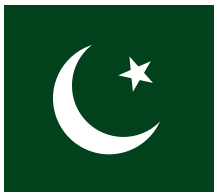
Pakistan

Print Pakistan



Last updated : 12/05/2020

Status regarding Budapest Convention

Status : NA

SEE LEGAL PROFILE

Cybercrime policies/strategies

The Government of Pakistan has not yet adopted a cybercrime strategy. A National Cyber Security Council Bill, 2014, which seeks establishment of a National Cyber Security Council and defines its functions and powers as to develop and draft policy, guidelines and governance models related to emerging cyber security threats has been tabled before the Senate. The government has approved e-mail and internet policy which envisages security guidelines and a multi-stage information security audit of government institutions and ministries.

Cybercrime legislation

State of cybercrime legislation

The Prevention of Electronic Crimes Act, 2016, is the main source of substantive law provisions, addressing in some form majority of the offences listed in the Budapest Convention.

The Prevention of Electronic Crimes Act addresses procedural powers corresponding to the Budapest Convention; however, several powers are missing procedural conditions and safeguards.

Substantive law

The Prevention of Electronic Crimes Act includes the following crimes: unauthorized access

to information system or data (Section 3), unauthorized copying or transmission of data (Section 4), interference with information system or computer data (section 5) , glorification of offences (section 9), cyber terrorism (Section 10), hate speech (Section 11), recruitment, funding and planning of terrorism (Section 12), electronic forgery (Section 13), electronic fraud (Section 14), making, supplying or obtaining devices for use in offence (Section 15), identity crime (Section 16) unauthorized interception (Section 19), defamation (Section 20), special protection of women (Section 21), child pornography (Section 22), writing or distributing malicious code (Section 23), cyberstalking (Section 24), spamming (Section 25) and spoofing (Section 26). The Prevention of Electronic Crimes Act also provides for legal recognition of offences committed in relation to information systems (Section 27).

In addition, the Penal Code also includes pornography (Section 292) http://jamilandjamil.com/?p=1052 while the Copyright Ordinance includes infringement of copyright (Section 66).

Procedural law

Although the main general framework applicable to all cybercrime investigations is the Code of Criminal Procedure (http://www.oecd.org/site/adboecdanti-corruptioninitiative/39849781.pdf), the Prevention of Electronic Crimes Act also includes specific procedural measures, applicable to all the investigations related to cybercrime, to crimes committed by the means of computer systems and to all the criminal investigations where digital evidence is required.

The Prevention of Electronic Crimes Act provides powers for expedited preservation and disclosure of data (Section 31), warrant for search and seizure (Section 32), power to conduct search and seizure (Section 35), conditions and safeguards with respect to search and seizure (Section 36), and real-time collection and recording of data (Section 39)

Safeguards

General rules and safeguards apply. In particular, the Prevention of Electronic Crimes Act provides limitations of scope and duration of exercise of powers (Section 18) as well as grounds for such exercise and independent oversight have also been included to a certain extent. However, the Prevention of Electronic Crimes Act allows investigators to not only seek preservation of data but also acquire data without a warrant where there is a risk or vulnerability that the data may be modified, lost, destroyed or rendered inaccessible (Section 31). Investigators also have an unqualified power to order any person in

possession of decryption information to grant access to a data, device or information system (Section 35).

Related laws and regulations

Besides an extensive legal framework on technical aspects, there are important acts on this field respecting:

- Electronic Transactions Ordinance 2002 (http://jamilandjamil.com/?p=938);
- Payment Systems and Electronic Fund Transfer Act, 2007 (http://www.sbp.org.pk/psd/2007/EFT_ACT_2007.pdf);
- Pakistan Telecommunications (Re-organization) Act 1996 (http://jamilandjamil.com/?p=936)

Specialised institutions

The Federal Investigation Agency has been designated as an investigation agency for the purposes of the Prevention of Electronic Crimes Act and it has the mandate to investigate and prosecute cybercrimes and crimes committed using electronic means. The trial of such cases is to be conducted by the Court of Sessions and higher courts where the presiding judge has successfully completed training with respect to computer sciences, cyber forensics, electronic transactions and data protection (Section 44).

The telecom companies' activities are regulated by the Pakistan Telecommunication Authority, which also has the mandate to block unlawful online content under the Prevention of Electronic Crimes Act (Section 37).

International cooperation

Competent authorities and channels

Legal Framework

Regarding internal law, Pakistan cooperates with other countries based on being a member of Interpol however such cooperation is on an ad hoc basis. Pakistan's Extradition Act governs the extradition process. Pakistan also has an extradition treaty in place with the United States of America which would be useful for cybercrime cases.

The Prevention of Electronic Crimes Act provides general international cooperation measures, including broad provisions relating to spontaneous information, grounds for refusal, confidentiality and limitation of use and enabling powers to cooperate with respect to specialized investigative measures (Section 34).

Competent authorities and channels

The legal competence to begin and direct criminal investigations belongs to the National Response Centre for Cyber Crimes (NR3C) of the Federal Investigation Agency. Under the Prevention of Electronic Crimes Act, the Federal Government is the competent authority with respect to sending and receiving international cooperation requests.

Jurisprudence/case law

There is no jurisprudence or case law with respect to the same.

Sources and links

- Country profile on cybercrime legislation for Pakistan: Profile 03/2010, in English, Profile 03/2010, in Urdu
- National Response Centre for Cyber Crimes (NR3C) http://www.policiajudiciaria.pt/PortalWeb/page/
- Pakistan Telecommunication Authority http://www.pta.gov.pk/index.php?Itemid=1