

The Prevention of Electronic Crimes Ordinance 2007

Current Status of the Bill

The Prevention of Electronic Crimes Ordinance 2007 was promulgated on December 31, 2007 by the then-President, Pervez Musharraf, by way of Presidential Ordinance LXXII. The ordinance has been re-promulgated on a number of occasions and is currently being reconsidered by the National Assembly Standing Committee on Information Technology & Telecommunication.

About Legislative Brief

This Brief is a part of PILDAT's Legislative Development Programme. The objective of the Brief is to assist parliamentarians to understand the context, objective and issues relating to the ordinance and to enable them to participate in a more informed debate and take well-considered position on the subject. The Brief is also intended to enhance awareness of the Citizens and Media in general so that they may also participate in the process as informed stakeholders and communicate their views to the public representatives. A broader objective is to make the legislative process open and participatory. The analysis and views contained in this Brief are not necessarily shared by the Friedrich Ebert Stiftung - FES.

Highlights of the Ordinance

The Ordinance comprises 49 sections and aims to criminalise various activities involving the use and misuse of electronic data, equipment and systems. The key features of the Ordinance include:

- The criminalisation of unlawful access and damage to and misuse of electronic data, equipment and systems
- The criminalisation of the creation and spread of computer viruses
- The introduction of an offence of cyber stalking
- The introduction of offences of spamming (sending bulk unsolicited mails) and spoofing (creation and use of fictitious websites)
- A provision criminalising "cyber terrorism"
- The establishment of exclusive investigatory and prosecutorial powers in the FIA
- The establishment of a specialist Information and Communication Technologies Tribunal; and
- Provisions relating to international cooperation with foreign Governments and agencies

Executive Summary

The Ordinance was a response to the growing problems arising from the use of computer data and systems in criminal activities both within Pakistan and internationally. The Ordinance builds upon existing provisions contained in the Pakistan Penal Code (PPC) and the Electronic Transaction Ordinance 2002. It is intended to cover existing crimes, which are carried out using electronic systems, and new offences, specific to electronic means. The provisions were introduced by the then-President, Pervez Musharraf, by way of Presidential Ordinance LXXII in December 2007. It has been re-promulgated on a number of occasions and is currently being reconsidered for further re-promulgation. The Ordinance essentially creates a number of criminal offences involving the misuse of electronic data, equipment and systems and the use of such data and equipment in the commission of other crimes. The sole power to investigate and prosecute offences under the Ordinance is vested in the Federal Investigation Agency (FIA). A new Tribunal, the Information and Communication Technologies Tribunal, was established to try cases under the Ordinance, the rules for which may be notified by Federal Government via the official Gazette. The Ordinance has been criticised on a number of grounds. The main concern remains that the offences outlined are vaguely defined, despite involving complex technological issues and carrying severe penalties. The media has noted with concern the offence of "cyber-terrorism," which is again very broadly defined and carries a potential death sentence. Concern has also been expressed as to the potential overlap of offences within the Ordinance itself and existing provisions contained in the PPC. The ability of the FIA to properly investigate matters involving such complex technological areas and, in particular, the ability of the FIA to ensure the data and hardware security of victims of electronic crimes has also been raised as a concern.

The Prevention of Electronic Crimes Ordinance 2007

The Position in India and Sri Lanka

Both India and Sri Lanka have invested heavily in information technology and outsourcing and both have legislated in relation to computer related crime: India in 2000 and Sri Lanka in 2007. India's legislation is broad, covering data protection, the legal standing of electronic signatures etc, along with computer crime. The computer crime sections were significantly amended in 2008 following recommendations from an advisory committee set up under the Act. The criminal offences covered are similar to those in the Ordinance, including cyber terrorism. Sri Lanka's Computer Crimes Act deals with similar computer related and hacking offences. The Act establishes a panel of experts to support criminal investigations and prosecutions. Both systems recognise the need for expert input in an area requiring detailed technical knowledge and rapidly changing technology.

Analysis of the Bill

Offences

Chapter II outlines a number of offences encompassing criminal access to any electronic system or device (section 3), criminal access to data using a system or device (section 4) and causing intentional damage to data or systems (sections 5 and 6). Section 7 sets out the offence of electronic fraud, which is defined as the use of electronic data, systems or devices with intention to deceive and cause damage or harm. Concern has been raised that this offence duplicates the existing offence relating to fraud set out in the PPC. Similar concerns have been raised in relation to section 8, relating to electronic forgery.

Unauthorised disclosure or access to codes, passwords and systems (section 10) and misuse of encryption to commit or conceal an offence (section 11) are criminalised. A new offence of malicious code is set out at section 12. This offence essentially encompasses the creation and distribution of computer viruses with the intent to cause harm or having the effect of causing damage to data. An exception is made for authorised uses in testing and designing systems.

Section 13 sets out the offence of cyber-stalking. This offence encompasses a number of distinct scenarios involving the intention to coerce, intimidate or harass by:

- i. Communicating obscene language or images
- ii. Making obscene proposals
- iii. Threats of illegal or immoral acts
- iv. Taking pictures without permission
- v. Displaying or distributing information which increases the risk of harm to another

The offence is very broadly and imprecisely defined and is capable of covering offences ranging from unauthorised

photography to blackmail whilst attracting a prison sentence of seven years or Pak Rs. 300,000 fine.

Sections 14 and 15 set out new offences of transmitting spam and "spoofing" (the creation of counterfeit websites or messages with intent to gain). Section 16 prohibits unauthorised interception of electronic data. Importantly it does not require any element of intent. In the absence of a malicious intention requirement this section gives rise to concern in relation to the use of Bluetooth devices, which intercept data from other Bluetooth enabled devices and may, therefore, attract liability.

The new offence of cyber terrorism is set out in section 17. This offence is highly controversial. It criminalises the use of any computer in any terroristic act with terroristic intent. Terroristic intent encompasses the intention to frighten, disrupt, harm, damage or be violent towards any segment of the population or Government entity. Terroristic act is very broadly defined, including but not limited to, altering information to cause injury or death, disrupting Government networks, aiding acts of violence and stealing or copying classified information or information relating to weapons of mass destruction. This offence is extremely broadly drafted and would appear to add an additional offence to various existing offences simply by the use of a computer (e.g. by sending an email). This offence, when causing death, is punishable by death or life imprisonment. Also controversial is the inclusion of an enhanced punishment, of up to 10 years imprisonment, in respect of offences involving sensitive electronic systems. Sensitive electronic systems include systems involving security/defence, confidential sources in criminal law enforcement, communications, banking, public utilities, courts, transport and emergency services. This provision includes a reversed burden of proof, under which knowledge of sensitivity

The Prevention of Electronic Crimes Ordinance 2007

is assumed unless otherwise proved. This provision is contrary to the basic principles of a fair trial and contravenes a number of international standards in relation to the conduct of criminal trials.

Procedures for Prosecution and Trial

The Ordinance places jurisdiction for investigation and prosecution of offences with the FIA, which is required to establish a special cell. Officers have powers, subject to obtaining a search warrant, to access and inspect systems, search for data, access codes and de-encryption, and to demand the assistance of a person with control of the system to access such information. A person who fails to comply may face charges of obstruction (section 26(3)).

Licensed service providers can be required to collect and record data and to retain data for a minimum of ninety days (sections 27 and 28).

The Ordinance creates an exclusive jurisdiction for a new tribunal, the Information and Communication Technologies Tribunal, whose members are appointed by Federal Government (without consultation with the Chief Justice or others) and whose principal seat is in Islamabad, with provincial benches made up of a minimum of two members. Minimum membership criteria require 10 years' High Court experience, two years' as a District of Sessions judge or ten years' specialist knowledge. The Tribunal has powers in relation to appeals from decisions of the Pakistan Telecommunications Authority and Electronic Certification Accreditation Council. Appeals from the Tribunal itself may be made to the High Court within thirty days of a decision. Parties before the Tribunal are entitled to legal representation and a panel of *amicus curiae* is established to assist the Tribunal with technical expertise where appropriate. In addition to the criminal penalties available, the Tribunal has a power to award compensation.

International Cooperation

The Federal Government is empowered to cooperate with foreign governments and international agencies in evidence collection, investigations and proceedings and to provide disclosure of material.

Weaknesses of the Current Legislation

The current Ordinance is subject to the following criticisms:

Extra-territorial Jurisdiction: The Ordinance covers offences committed both inside and outside Pakistan, having a detrimental effect on the security of Pakistan, its nationals or

national harmony, or any property, data or system either located in Pakistan or capable of being connected to, sent to, or used by or with any system in Pakistan. Given the potential connectivity of devices and data internationally, this essentially creates liability for offences committed abroad, by both Pakistani and non-Pakistani citizens, with no connection to Pakistan. Other jurisdictions require a "significant link" to the state concerned. Whilst international jurisdiction does appear in various legal systems, it is generally reserved for the most serious offences, such as murder, torture and war crimes.

Definitions: A number of the definitions adopted are complex and wide. The definition of electronic device, for instance, encompasses any electrical equipment. Definitions of cyber-stalking and terroristic acts are very wide and will give judges considerable discretion in interpreting the scope of the offences. Given the heavy penalties concerned, such discretion is inappropriate.

Unauthorised Interception: This offence currently does not require any element of intention and could therefore encompass accidental/unintentional and harmless interception, particularly through the use of Bluetooth devices. As Bluetooth devices are designed to intercept other Bluetooth enabled devices the absence of malicious intention will criminalise even benign interceptions.

The Reversed Burden of Proof: The provision on sensitive electronic systems reverses the burden of proof, requiring the accused to demonstrate lack of knowledge of sensitivity. This provision runs against international norms which require the burden of proof in criminal matters to rest with the prosecution.

Duplication of Offences: There is a significant risk that a number of offences duplicate offences set out elsewhere, in particular section 4 appears to necessarily involve the commission of a section 3 offence and it appears that the offences of fraud and forgery, as defined elsewhere in the PPC, would be committed along with sections 7 and 8, thus creating dual liability for any single offence. However in other jurisdictions lacunae have been identified in existing fraud and forgery offences requiring specific legislation. These difficulties arise from the requirement of "deception" and the view that computer data is not property. The UK courts, for instance, have taken the view that as a computer is not capable of thought it cannot be deceived and that various fraud and forgery allegations fail if effected using a computer. It would be necessary to draft specific offences to deal with such difficulties or to make clear that duplicate charges cannot be brought.

The Prevention of Electronic Crimes Ordinance 2007

Recommendations

1. That the jurisdictional definition of offences be amended to require a significant link to Pakistan
2. That the definition of electronic devices be amended to as to make clear that such devices, to be covered, are capable of communication
3. That the offences of cyber-terrorism and cyber stalking are more narrowly defined so as to remove the possibility of judicial discretion in interpretation
4. That the offence of unauthorised interception is amended so as to include a requirement of malicious intent
5. That the reversed burden of proof in relation to sensitive electronic systems be removed
6. That the Ordinance be amended to make clear that no person may be prosecuted under both the Ordinance and PPC/other legislation in respect of the same alleged offence
7. That measures are put in place in relation to capacity building amongst the relevant cell of the FIA and the Tribunal panel members so as to ensure that they are adequately trained
8. That measures be included to safeguard the integrity of hardware and data accessed or seized during any investigation and that confidentiality of data be ensured

National Assembly Standing Committee on Information Technology & Telecommunications

1. **Ch. Muhammad Barjees Tahir, Chairman** (NA-135, PML-N)
2. **Malak Azmat Khan** (NA-34, PPPP)
3. **Mr. Muhammad Faiz Tamman** (NA-61, PML-N)
4. **Sardar Talib Hassan Nakai**, (NA-142, PML)
5. **Chaudhry Iftikhar Nazir**, (NA-159, PPPP)
6. **Khawaja Sheeraz Mehmood**, (NA-171, PPPP)
7. **Mr. M. Mohsin Ali Qureshi**, (NA-176, PML)
8. **Syed Muhammad Saqlain Bukhari**, (NA-182, PML-N)
9. **Mr. Ghulam Murtaza Khan Jatoi**, (NA-211, NPP)
10. **Mir Munawar Ali Talpur**, (NA-227, PPPP)
11. **Dr. Talat Iqbal**, (NA-233, PPPP)
12. **Mr. Roshan-ud-Din Junejo**, (NA-236, PPPP)
13. **Mr. Sajid Ahmad**, (NA-257, MQM)
14. **Justice (R) Fakhar-un-Nisa Khokher**, (RS, Women, PPPP)
15. **Mrs. Farhat Khan**, (RS, Women, PPPP)
16. **Mrs. Anusha Rehman Khan**, Advocate (RS, Women, PML-N)
17. **Ms. Marvi Memon**, (RS, Women, PML)

For communicating your views to the committee, you can contact:

Secretary National Assembly Standing Committee on Information Technology & Telecommunication

C/O

Secretary,

National Assembly of Pakistan

Parliament House,

Islamabad

Ph. +92-51-920-3734, +92-51-922-1082

Fax: +92-51-920-4673, +92-51-922-1106

E-Mail : assembly@na.gov.pk