Electronic Crimes Ordinance: An Overview of Its Preamble and Extent[1]

Muhammad Amir Munir

The opening para of the Prevention of Electronic Crimes Ordinance reads as under:

> **WHEREAS** it is expedient to prevent any action directed against the confidentiality, integrity and availability of electronic system, networks and data as well as the misuse of such system, networks and data by providing for the punishment of such actions and to provide mechanism for investigation, prosecution and trial of offences and for matters connected therewith or ancillary thereto
>
> AND whereas the National Assembly stands dissolved and the President is satisfied that the circumstances exist which render it necessary to take immediate action:
>
> Now, therefore, in exercise of the powers conferred by clause (1) of Article 89 of the Constitution of the Islamic Republic of Pakistan and in exercise of all powers enabling in that behalf, the President is pleased to make and promulgate the following Ordinance:-

Commentary

Almost 30 years ago, on August 1, 1978, the Florida Computer Crimes Act (Chapter 815, Florida Statute) came into force. Its *preamble* described the importance of the issue of computer crimes in the words:[2]

> **"Fla. Stat. 815.02 Legislative Intent**
>
> The Legislature finds and declares that:
>
> i. Computer-related crime is a growing problem in government as well as in the private sector.
>
> ii. Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime.
>
> iii. The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets, are great.

iv. While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse."

Likewise, the United Kingdom passed the Computer Misuse Act in 1990 when many problems relating to computer crimes came on record but courts found it difficult to convict accused of new generation of crimes. For example, prior to this law, cases were decided under the Theft Act of 1968 and 1978, the Criminal Law Act, 1977, the Criminal Attempts Act, 1981, the Forgery and Counterfeiting Act, 1981, the Data Protection Act, 1984, the Criminal Damage Act, 1971, the Trade Description Act, 1968, the Interception of Communications Act, 1985.[3]

The difficulty for courts and prosecution for curtailing the computer related crimes is seen in a number of cases that were decided prior to the enactment of the 1990 Act. In *DPP v. Ray,* [1974] AC 370, a case of deception under the Theft Act, 1968, it was held by the House of Lords that "for a deception to take place there must be some person or persons who will have been deceived." In *R v. Gold,* [1988] 2 WLR 984, the conviction by the Crown Court under the Forgery and Counterfeiting Act, 1981 for hacking the computer password was reversed by the Court of Appeal and House of Lords. In *Oxford v. Moss*, (1978) 68 Cr App R 183, it was held that confidential information does not come within the definition of property for the purpose of theft.

On the other hand, it was held in *Cox v. Riley*, (1986) 83 Cr App R 54, that the accused has damaged the printed circuit card although the accused argued that he has not damaged any tangible property within the meaning of the Criminal Damage Act, 1971. Further, in *R v. Whiteley*, (1991) 93 Cr App R 381, the accused who gained unauthorized access to a system where he added and deleted files, changed passwords and deleted audit files recording his activities, was convicted for the charge of damaging computer disks. His argument that no tangible damage has been caused was rejected by the Court of Appeal holding that the 1971 Act require damage to tangible property and not that the damage itself should be tangible.

Considering all these problems and prospects of an overcrowding generation of computer related crimes, the Computer Misuse Act, 1990 was enacted with the following Preamble:[4]

"An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes."

Malaysia also took lead by enacting the Computer Misuse Act, 1997 (Act 563).[5] The Preamble to this law reads:

"An Act to provide for offences relating to the misuse of computers."

This is a small legislation that defines five distinct offences (ss. 3 to 7) relating to computer misuse.

India also enacted the relevant legislation in the year 2000 when it passed the Information Technology Act, 2000. *Preamble* to this Act reads:

> " An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.
>
> whereas the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;
>
> and whereas the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-cased methods of communication and storage of information;
>
> and whereas it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records."

It seems that Indian legislature was more concenred with the electronic commerce and its recognition as compared to electronic crimes because the emphasis of the *Preamble* is on electronic commerce and communication. Nowhere we found the reference to electronic or cyber crimes in this Preamble. However, this legislation is comprehensive and covers substantially the issues of digital signatures and electronic or cyber crimes. For example, Chapters IX and XI deal with issues of computer crimes.

The scenario in Pakistan is little different. Pakistan adopted an un-planned step by step approach starting through an amendment in copyright law in 1992 and leading towards the present specific legislation on the issue of electronic crimes enacted on the last day of the year 2007. It was in the year 1992 when the first computer related amendment in the law was made in the Copyright Ordinance, 1962 when the term "literary work" was expanded to also include 'computer programs' as one of the kinds of "literary work".[6] Thus any infringement of copyright law relating to computer programs was made adjudicable both at civil and criminal sides.[7]

The Copyright Ordinance, 1962 provides both civil and criminal remedies for any alleged infringement of copyrights. Thus anyone who unauthorizedly copies a computer program or software may be held liable for civil and criminal liabilities.[8] However, it is to be seen if any computer program infringement matter has been decided by the superior courts and reported accordingly in various law reports.

At criminal side, there was no legislation that specifically encircled the electronic data theft problems. Section 22 of the Pakistan Penal Code, 1860 defines the term 'movable property' as under:

22. "Movable Property"

The words "Movable Property" are intended to include *corporeal*[9] property of every description, except land and thing attached to the earth or permanently fastened to anything which is attached to the earth".

Here the word "corporeal" is of much significance as the electronic data or electronic document does not fall under the meanings of this word. Further, the dictionary meaning of the term 'property' also suggest that it is something tangible and can be possessed. At the same time, the word "document" defined in section 29 of the 1860 penal code was also exclusive of electronic documents and data. It reads as under:

"**29. "Document"**

The word "document" denotes any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, as evidence of that matter.

Explanation 1

It is immaterial by what means or upon what substance the letters, figures or marks are formed, or whether the evidence is intended for, or may be used in, a Court of justice, or not.

Explanation 2

Whether it is expressed by means of letters, figures or marks as explained by mercantile or other usage, shall be deemed to be expressed by such letters, figures or marks within the meaning of this section, although the same may not be actually expressed."

In this definition, word 'substance' is relevant for our discussion. This word is not defined in the penal code and hence we have to look into the dictionary meaning. According to the *Merriam-Websters',* 11th edition, substance means a physical material from which something is made. Hence, these two important definitions in the penal code were not comprehensive in their original form to include electronic

documents or electronic data or property that is available only in electronic format like a document prepared and saved in hard disk of a computer but never printed. In today's understanding, it (e-data or e-document) *is* a property against which a particular act or omission may be an offence. So these laws were required accordingly to be modified. Otherwise, before the enactment of present law, if a person steals a computer, he may be charged with the offence of theft but if he only steals the whole data saved in its hard disk by means of copying while leaving the original data unchaged, perhaps he could not be charged of any offence.[10]

The advent of internet and world wide web also added more complexities in this regard. A person cannot even be held liable for cheating if he deceives a computer or a system (machine) as the cheating is to be done by a person against another person. Further, physical presence has also become irrelevant at the scene of crime as a computer expert sitting in one part of the world can deceive another computer system in some other part of the world by sending an executable program to that system. Pakistan has faced many such problems but as there was no clear law or policy in this regard and as there was less awareness about the computer crimes, most of the issues remained unnoticed or unreported to the police in the past.

At the same time, another area that experienced notable growth was electronic commerce.[11] As it is becoming the norm to use electronic means for business transactions, therefore, a heavy mass of big transactions of business got attention of all stakeholders in Pakistan and hence efforts were made to regulate the electronic commerce. In the year 2002, the Electronic Transaction Ordinance, 2002 (*hereinafter* ETO, 2002) was promulgated. The operative part of its *Preamble* reads as under:[12]

> "to recognize and facilitate documents, records, information, communications and transactions in electronic form, and to provide for the accreditation of certification service providers.
>
> WHEREAS it is expedient to provide for the recognition and facilitation of documents, records, information, communications and transactions in electronic form, accreditation of certification service providers, and for matters connected therewith and ancillary thereto;".

Resultantly, a number of changes were made in other laws dealing with 'documents' and full recognition was given to e-documents.[13] The Qanun-i-Shahadat Order, 1984 was also amended by this Ordinance and hence the evidentiary value was given to the electronically generated documents equal to the conventional documents.[14] The words "electronic", "electronic document" and "electronic signature" were defined and brought on statute book of Pakistan.[15] Section 30

ETO, 2002 comprehensively gives cover to most of the documents that can be generated through electronic means.

Cyber crimes' were also recognized in the ETO, 2002 wherein unauthorised access and damage to any information system were made offences punishable with imprisonment and heavy fine.[17] These were the only enabling provisions of law since the year 2002 uptil now under which the computer offences were made cognizable. Section 58 of the Payment Systems and Electronic Fund Transfers Act, 2007 (IV of 2007) defines the offence of Cheating by Use of Electronic Device. Earlier on, section 31 of the Pakistan Telecommunication (Re-Organization) Act, 1996 (XVII of 1996) defined a number of offences that generally fall under the definition of cyber or electronic crimes.

After promulgation of the Prevention of Electronic Crimes Ordinance, 2007 (*hereinafter* PECO, 2007), the offences defined in the Ordinance are to be tried by a special Tribunal that will be constituted by the government. The offences defined in laws mentioned in Schedule to this Ordinance shall also be tried by the Tribunal. Further, this law has over-riding effect and hence any provisions in existing laws contrary to this Ordinance shall have no effect. The Tribunal under this Ordinacne has yet to be notified by the government and hence till establishment of the Tribunal, the transitory provisions of this Ordinance provide that the law will be administered by the competent forums under existing laws.

Even at this moment, no Rules have been prescribed by the government as required under this Ordinance.

The Extent of Law and its Application

1. Short Title, Extent Application and Commencement.-

i. This Ordinance may be called the Prevention of Electronic Crimes Ordinance, 2007.[18]

ii. It extends to the whole of Pakistan,

iii. It shall apply to every person who commits an offence under this Ordinance irrespective of his nationality or citizenship whatsoever or in any place outside or inside Pakistan, having detrimental effect on the security of Pakistan or its nationals or national harmony or any property or any electronic system or data located in Pakistan or any electronic system or data capable of being connected, sent to, used by or with any electronic system in Pakistan.

iv. It shall come into force at once,

Commentary

As the Pakistan Penal Code, 1860 (hereinafter PPC) is 'general'[18] penal law, therefore, for any special kind of offences or crimes a special law can be enacted by the legislature.[19] Considering the importance and uniqueness of the cyber or 'electronic crimes, the present law was enacted through an Ordinance. Under this law, 'jurisdiction' is one of the most important questions to be determined by the courts. Being a new legislation under the cyber regime, where physical state boundaries have no meaning as far the netizens[20] are concerned, much law will develop on the issue of jurisdiction because it is now norm, and not the exception, that people who are non-citizens and who are sitting in another country are causing cyber crimes in different jurisdictions. The matters relating to jurisdiction, evidence and extradition are part of major discussions regarding international treatise on the subject of cyber crimes. For example, the Budapest Convention[21] of 2001 on Cyber Crimes, have special provisions relating to jurisdictional matters and international cooperation in this regard.

Jurisprudentially, it will not be out of question to remind the readers that the PPC's approach already caters generally for the issue of commission of offences (defined under Pakistani laws) by non-citizens in jurisdictions beyond Pakistan. Sections 3 and 4 of PPC are most relevant in this regard. For ready reference, they are reproduced here, *mutatis mutandis*, as under:

"3. Punishment of offences committed beyond, but which by law may be tried within Pakistan.

Any person liable, by any Pakistan Law, to be tried for an offence committed beyond Pakistan shall be dealt with according to the provisions of this Code for any act committed beyond Pakistan in the same manner as if such act had been committed within Pakistan.

"4. Extension of Code of extra-territorial offences.

The provisions of this Code apply also to any offence committed by:--

i. any citizen of Pakistan or person in the service of Pakistan in any place without and beyond Pakistan

ii. Omitted

iii. Omitted.

iv. any person on any ship or aircraft registered in Pakistan wherever it may be.

Explanation

In this section the word "offence" includes every act committed outside Pakistan which, if committed in Pakistan, would be punishable under this Code."

Explanation to section 4 of PPC is most relevant in this respect read with illustration at letter (d) in this section. This illustration is quoted here *verbatim*:

"(d) *D,* a British subject living in Junagadh, instigates *E*, to commit a murder in Lahore. *D* is guilty of abetting murder."

Here, the subject is a foreigner (British subject), living in another country (India) and committing an offence that is to be done in Pakistan by a third person. Still, he or she can be charged with the offence of abetting murder.

The restricted provision of PPC is section 2. It reads as under:

"2. Punishment of offences committed within Pakistan, etc.

Every person shall be liable to punishment under this Code and not otherwise for every act or omission contrary to the provisions thereof, of which he shall be guilty within Pakistan."

In an old case, it has been held by the Lahore High Court that s. 2 must be read subject to s. 5 which clearly makes a reservation with regard to offences specified therein.[22]Therefore, only those offences which are mentioned in general penal code (PPC) or any local or special laws are punishable.[23] An early case in this regard decided by the Indian Supreme Court provides that where a foreigner by false representations made by post from a foreign country to a Pakistani living in Pakistan, defrauds him of his property, he can be held guilty under the Penal Code notwithstanding the fact that he was a foreign national at the time when he made those representations and committed the offence.[24] The intra-territorial application defined by s.2 PPC will be no bar on extra-territorial application of PECO, 2007 because of the fact that special penal laws can be enacted in accordance with s.5 of PPC.[25] These interpretations of general penal law provide a strong backbone for enforcement of special law like the PECO, 2007.

However, to implement these provisions or provisions of this Ordinance regarding extended jurisdiction to local courts will remain a big jurisprudential debate in the courts. We have to wait for development of the law in this regard to be propounded by the superior courts while interpreting the newly enacted legislation to explain it further. Of course, the answer in this regard will be to study none else than international cooperation in this regard. The Budapest Convention, as also the present law, contains special provisions of international cooperation in combating cyber crimes and related issues. States are required to remain in close contact and cooperation in such type of matters where extradition involves. Some countries may not allow their citizens to be extradited only for the reason that said person or persons have committed a cyber offence and caused serious damage to the systems in requesting country. Further, definition of an offence and its gravity may be different from jurisdiction to jurisdiction. May be an act is an offence in one country

and not in another! Still, the country of offender may not follow a particular definition of another country of an act or omission classified as an offence. These are complex legal issues that will require all the legal actors (judges, magistrates, attorneys, law teachers, law officers, public prosecutors, defence lawyers, investigators, police etc.) to move ahead with more knowledge and understanding of the issues through use of relevant literature available in print and cyber media. Likewise, universities and law schools need to evolve a strategy to provide academic backbone on the issue by conducting relevant research and writing and publishing of indigenous materials.

Another relevant question may arise about the application of principle of *Ignorantia Legis Neminem Excusat* (ignorance of law excuses nobody)[26] to the netizens. Section 79 of PPC reads as under:

> **"79. Act done by a person justified, or by mistake of fact believing himself justified, by law.**
>
> Nothing is an offence which is done by any person who is justified by law, or who by reason of a mistake of fact and not by reason of a mistake of law in good faith, believes himself to be justified by law, in doing it."

How the courts will presume that the offender was, in fact, in knowledge of any particular law defining an act or omission as an offence in a particular jurisdiction where he/she had never physically gone or about which he/she had no information; but in physical territory of said jurisdiction he/she had done an act which constitutes an offence there? A difficult and complex question may arise when the offender takes the plea or defence of innocence regarding a factual mistake about law.[27] In India, Supreme Court has held that for an Indian law to operate and be effective in the territory where it operates namely, the territory of India, it is not necessary that it should either be published, or be made known outside the country.[28] Further, the Gazette published by the government is not yet issued electronically in all jurisdictions. The consequence of such type of ignorance may result in mitigating the sentence and not the benefit of the maxim of ignorance of law as an absolute defence.[29] An old English case is referred in this regard universally. It is *R.* v. *Bailey* (1800), Russ & Ry. 1, 168 E.R. 651. In a Canadian case cited *R. v. Campbell and Mlynarchuk, (1973), 10 C.C.C. (2d) 26*, District Judge Kerans elaborates *Bailey* in the following words:[30]

> "Well, I have already indicated, in a quotation from Kenny, that, in this awkward situation, the matter does not afford a defence, but should certainly be considered in mitigation of sentence. Indeed, there are several cases, not as awkward as this, in the law reports, involving a person who had an honest and reasonable mistake in belief as to the law, and for whom the Courts expressed sympathy, and, in respect of whom, sentence was mitigated.

> It is at this stage where the scales of justice are balanced. Clothed with very recent power to refuse to enter a conviction, I can now balance the scales of justice even more delicately. I have read a note in vol. 14 of the English and Empire Digest, at p. 51 of an old case, *R*. v. *Bailey* (1800), Russ & Ry. 1, 168 E.R. 651. It goes back to 1800. In that case, the Government of England had passed a statute, making something a crime which was not previously a crime. Subsequently, the accused did the forbidden act. The Courts found that, in fact, in the district in which this crime was committed, no news had yet reached anyone of the passage of this *Act*. Nor could any news have reached this district of the passage of this *Act*. And that the accused, therefore, had to be convicted of an offence which he did not and could not have known was an offence. And they said there that the proper way of dealing with the matter was to give a pardon, which I understand to be a conviction followed immediately by the wiping out of a conviction.
>
> I have no power to give a pardon, but I do have power to give an absolute discharge. In my view, this is the proper case."

This being the position, it is important to revisit the principles laid down in *Bailey* so that prospective criminals may not get an unnecessary advantage of mitigating circumstances for a lesser sentences in this era of information technology.

At the moment, not much law is developed under section 79 of PPC though with few reported cases, it is settled that the Courts in Pakistan do not accept the plea of mistake of law as an absolute defence.[31] However, with the promulgation of the present Ordinance, if foreigners as accused are brought to the courts of Pakistan, there are chances of excessive defence plea under this provision and may be courts are required to adopt a moderate version of *Bailey*!

Another area of reasonable consideration is the fact that juveniles are most vulnerable to cyber / electronic crimes because of computer learning starting from early years of their education. Now a day, access to internet has become the easiest. There are many possibilities that a young computer programmer (under 18 years or even under 15 years)[32] sitting in another country enters into the critical systems of Pakistan and commits an act which is an offence[33] under the present Ordinance. The delicacy and issues of juvenility and proof of criminal intent are going to be the complex legal issues for the judges of cyber crimes courts. In this respect, the PECO, 2007 is required to be read with the Juvenile Justice System Ordinance, 2000 and sections 82 & 83 of the PPC. A good example of warning students of a university[34] to avoid any misuse of cyberspace becomes relevant for educating our youth about prospective misuse or abuse of cyberspace or computer technology so that they can avoid any criminal proceedings. But what is for juveniles who are citizens of another country sitting in that country?

Juveniles may also become victims of cyber / electronic crimes. The present law defines crimes and punishments, and hence, this area is out of our discussion.

End Notes

[1]This study is made prior to the issuance of latest edition of the PECO 2009. However, it is considered that the provisions of the latest version are replica of earlier editions of this law. The reason of issuance of number of editions of this law is that the law was originally issued as a Presidential Ordinance which cannot last more than four months unless ratified by the Parliament. The Parliament is yet to enforce it as an Act of the Parliament.

[2]http://www.clas.ufl.edu/docs/flcrimes/subsubsection2_1_1_2_2.html. Visited on 2 February 2008.

[3]See generally, Bainbridge, David I., *Introduction to Computer Law*, 2nd Ed., London: Pitman Publishing, 1993, Parts III & IV.

[4]http://www.opsi.gov.uk/acts/acts1990/ukpga_19900018_en_1. Visited on 3 February 2008.

[5]http://www.msc.com.my/cyberlaws/act_computer.asp. Visited on 3 February, 2008. However, the law came into force on 1st June, 2000.

[6]See the Copyright (Amendment) Act, 1992 (XX of 1992).

[7]Civil remedies include injunction, damages, accounts and otherwise as are of may be conferred by law for the infringement of a right (s. 60). Every suit or other civil proceeding regarding infringement of copyright shall be instituted and tried in the Court of the District Judge (s. 65). All offences under the Copyright Ordinance,

1962 are triable by a court not inferior to that of a Magistrate of the first class (s. 72).

[8]See Chapters XIII & XIV of the Copyright Ordinance, 1962, as amended in 1992.

[9]Emphasis added by the commentator.

[10]See generally, Muhammad Amir Munir, "Electronic Crimes Act, 2004: The Proposed E-Law in a Judge's Perspective", in PLJ 2005 Magazine 333.

[11]See *Secrets of Electronic Commerce,* Lahore: The Small and Medium Enterprise Development Authority (SMEDA) & International Trade Center (UNCTAD / WTO), 2002. It provides wonderful reading on the subject of electronic commerce in Pakistan.

[12]http://www.fia.gov.pk/ETO.pdf. Visited on 18 February 2008.

[13]S. 3 of the ETO, 2002 reads: "3. Legal recognition of electronic forms. No document, record, information, communication or transaction shall be denied legal recognition, admissibility, effect, validity, proof or enforceability on the ground that it is in electronic form and has not been attested by any witness." See http://www.fia.gov.pk/ETO.pdf. Visited on 18 February 2008.

[14]It is pertinent to mention that already article 164 of the Qanun-e-Shahadat Order, 1984 provides production of evidence that has become available because of modern devices. However, this article could not be used to define new crimes or offences. It is only an enabling provision where existing offences and civil rights can be proved through evidence that has become available due to modern devices. Hence, the amendments introduced now have minimized the court discretion and uncertainty of admissibility of certain electronically generated documents in this regard and courts are now bound to give full evidentiary value to different electronically generated documents as per new amendments and letter of law.

[15]See s. 2 (l), (m) & (n) of the ETO, 2002. See http://www.fia.gov.pk/ETO.pdf. Visited on 18 February 2008.

[16]See sections 36 & 37 of the ETO, 2002. However, no case has yet been reported in law reports. But it does not mean that cases have not been registered or lodged under these provisions. In Pakistan, only those cases are reported in law reports which are decided by the superior courts. Further, as the offences so defined are compoundable and hence it is probable that the offenders use the opportunity to enter into compromise with the complainant and hence matter is not reached up to the superior court for interpretation or appeal/revision etc.

[17]Hereinafter may be referred as the PECO, 2007.

[18]*Preamble* to the Pakistan Penal Code (PPC) reads: "Whereas it is expedient to provide a *general* Penal Code for Pakistan…". (emphasis added)

[19]Section 5, PPC specifically provides that the Pakistan Penal Code will not affect, *inter alia*, any special law.

[20]This term can be used for those persons who use internet and cyberspace for any purpose. These are 'net citizens'. It may be a derivative of the term 'citizen' and may not yet be adopted by most of the English Language Dictionaries. However, *Merriam Webster's Collegiate Dictionary,* 11th Ed., (hereinafter referred to as 'Webster's') defines this term as "an active participant in the online community of the Internet." Further, if we google the word "netizen", some information is available to understand the term. See

http://www.columbia.edu/~hauben/text/WhatIsNetizen.html or http://en.wikipedia.org/wiki/Netizen for more discussion about this term. Sites visited on 7 August 2008.

[21]See Annexure.

[22]AIR 1929 Lah. 217.

[23]AIR 1921 Cal. 1.

[24]PLD 1958 SC (Ind) 115.

[25]It has been mentioned in *The Indian Penal Code* by Ratanlal & Dhirajlal, 29th Edition, Nagpur: Wadhwa Publishers, 2003, at p. 39 that "[t]he rule of intra-territorial or extra-territorial operation of the laws has undergone drastic changes in India, in view of the enforcement of the Information Technology Act, 2000."

[26]Dr. A. R. Biswas, *Encyclopedia Law Dictionary with Law Terms and Phrases Judicially Interpreted,* Lahore: Shan Corporation, nd. See also http://encyclopedia.thefreedictionary.com/Ignorance+of+the+law+is+no+excuse and Wikipedia websites. Sites visited on 7 August 2008.

[27]'Mistake of law' ordinarily means mistake as to the existence or otherwise of any law on a relevant subject as well as mistake as to what the law is. See *Tustipada Mandal,* (1950) Cut 75.

[28]*Mayer Hans George,* (1964) 67 Bom LR 583; AIR 1965 SC 722.

[29]*See* generally, AIR 1953 Punj. 227.

[30]Visit http://faculty.law.ubc.ca/benedet/casebook/casebook9%202007.doc. Site visited on 10 August 2008.

[31]On www.pakistanlawsite.com, only few cases have been mentioned under s.79, PPC.

[32]Section 2(b) of the Juvenile Justice System Ordinance, 2000.

[33]Section 2(f) of the JJSO 2000 defines the term 'offence' in following words: " 'Offence' means an offence punishable under any law for the time being in force."

[34]University of Virginia has published an online handbook titled "Responsible Computing at the UVa". This guides students of UVa about ethical uses of computer and cyberspace and cautions them about criminal proceedings in case of violations. This hand book can be accessed at http://itc.virginia.edu/pubs/docs/RespComp/rchandbook.html. Visited on 16 August 2008.

Conclusion

The above discussion reveals that the application of this law needs many delicate and new questions to be determined judicially. However, it is an important development at the statute book of Pakistan that the new types of crimes have been given due weight for their curtailment with reference to their spread without national or geographic boundaries. The above discussion is only to analyze only the nature and extent of law and few issues of its applicability to non-citizens or netizens especially when they are sitting beyond territorial jurisdiction of Pakistan. It is hoped that further discussion on the issue will help improvement not only in the law itself but also in its administration by the courts of law. Though this article did not discuss the issue of research on this law, but it is suggested that law schools and bars need to consider establishing cybercrime law centers so that they can provide academic backbone to the courts, lawyers, judges, legal academics, law students and other related organizations with respect to issues that this law has to address.

Muhammad Amir Munir is an LLB and LLM from Punjab University and is serving as Civil Judge 1st Class / Magistrate s.30, Islamabad. He has been writing on the issue extensively and has published in various national and international forums. It is also pertinent to mention that this study is part of a commentary that the author is preparing on PECO and is without any prejudice to author's official obligations and does not reflect the official stand of any body or organization. Author can be contacted at bionic4@hotmail.com.