CYBER LAWS IN PAKISTAN

Justice (R) Khalil-ur-Rehman Khan

1. Need for Cyber Laws

1.1. E-commerce, short for electronic commerce, is conducting business on-line, including buying and selling products with credit card or digital cash, by transfer of data between different companies using networks, such as the Internet. More precisely e-commerce is the collection of tools and practices involving Internet technologies that allow a company to create, maintain and optimize business relations with consumers and other businesses.

1.2. E-commerce penetrates into every corner of the modern business and with good reason. It promises reduced costs, higher margins, more efficient operations and higher profits. It is useful to both producers and consumers in developing countries as it helps them overcome the traditional barriers of distance from markets and lack of information about market opportunities. Producers and traders no longer need to maintain physical establishments requiring large capital outlays. Virtual shops and contract points on the Internet may enable storage close to the production site, and distribution can be made directly to the consumer. Increased advertising possibilities worldwide may help small and medium industries and businesses in developing countries, which traditionally find it difficult to reach the customer abroad. It may also enable such firms to eliminate middlemen while trying to sell their products abroad.

1.3. Trade and business communications through electronic means give rise to a number of legal issues. For instance if a service were sold over the Internet across countries, in which geographical location can the transaction be deemed to have occurred? This question may be important from the point of view of consumer protection and establishing jurisdiction. Furthermore electronic transactions require electronic contracts and electronic signatures which have not been provided for in the contract laws of many countries. Most countries that wished to participate in electronic commerce needed to undertake major legislative reforms in this regard.

2. E-Commerce in Shariah Perspective

2.1. Businesses find, thanks to Internet, limitless place in the cyberspace by providing easy access to potential customers all over the world without any limitation as to business hours and 24 hours a day, seven days a week for the whole year. It is easy to advertise products and commodities more satisfactorily and overall expenses are reduced by the use of Internet, so the contract entered into on Internet, to be enforceable and valid, must fulfill essential legal conditions prescribed by Shariah.

2.2. Contract formation over Internet

2.2.1. Unless any element that is prohibited by Shariah is involved, a contract formation over the Internet or in cyberspace is completely legal. An agreement enforceable by law is a contract. In principle, a contract must include a proposal, acceptance to the proposal and valid consideration.

2.2.2. Al-Qur'an[2] sanctifies by pronouncing "O ye who believe! Fulfill (all) obligations ('Uqud)". The singular of 'uqud is 'aqd in Arabic which means conjunction; tie, to tie between two ends of something either physically or morally.

2.2.3. In Islamic law, contract covers the entire field of a wide variety of obligations including those that are spiritual, social, political and commercial. More specifically, '*aqd* refers to the meeting of offer and acceptance in conformity with the formality prescribed by the Shariah.[3]

2.2.4. The contract formed on the Internet is an ordinary business contract with necessary modifications made in order to adapt to the cyberspace environment. The buyer and seller need not physically meet each other. They interconnect through the words they type on the keyboard; so it is an alternate paperless media communication in place of ordinary face to face communication or communication via telephone or facsimile or other communication facilities. What is needed is that there must be at least two parties acting as offeror and offeree. There must also be a valid offer accepted by a valid acceptance for a valid consideration as otherwise no contract enforceable at law comes into existence. Each requirement is indispensable for formation of contracts generally, without exception for those being formed over the Internet.

2.2.5. The special feature of a contract on the Internet is that problems may arise when the offeror asserts that his offer has lapsed while the offeree contends that he has executed an acceptance effectively. It is to be noted that in order to determine whether a contract has been concluded or not, it has to be proved that the offer was effectively accepted.

2.2.6. To avoid problems regarding acceptance, it is necessary that the offeror specify a period within which acceptance is to be received and in what manner. The general rule, that acceptance must be communicated, shall be given recognition for contracts formed in cyberspace. Due to its unique feature, any data message communication should be deemed to have been received when it has reached the information system of its intended recipient. It does not matter that the receipt is effected by a machinery system as opposed to a human being.

2.2.7. Hence it is strongly advisable that the offeror should include in his offer a provision requiring acknowledgement of receipt of offer. Hence he may presume the point in time after which he is free to transfer the offer to another party. This principle is based on the following tradition (Hadith):-

2.2.8. It was narrated by Abu Daud, Ibn Majah and Tirmizi from 'Amr Ibn 'Auf that Prophet (PBUH) said: "Amicable settlement is permissible for Muslims except a settlement to forbid what is permissible or to approve what is forbidden; and Muslims are bound by their conditions except the condition that forbids what is permissible or approves what is forbidden." See Wahbah Zuhayliy, Al-Fiqh al-'Islamiy, vol. 4 at 200. Further, it is stated that validity of contract, under Islamic contract law is subject to four classes of conditions. They are (i) conditions necessary as the basis for contract formation, e.g. to require that the subject matter of contract is to be delivered; (ii) conditions that are legally required for the validity of contract, e.g. the contract shall not involve *gharar*l (uncertainty); (iii) conditions necessary for enforceability of contract, e.g. the seller must have the ownership or legal title on the subject mater of contract; and (iv) conditions necessary to enable performance of contract, e.g. contract for sale shall be free from option, at 224-231. As requiring acknowledgement of receipt of data message communication does in no way contradict Islamic contract law principles, such condition is valid and enforceable.

[1] Section 10 Contract Act 1872
[2] Surah al-Maidah 5:1
[3] Wahbah Zuhayliy, Al-fiqh al-'Islamiy Wa Adillatuhu, vol. 4, 3rd ed..Damascus: Dar Al-Fkr, 1409H/1989M at 80-81. See also Art. 103 of the Mejelle and Art. 167 provides that "by an offer and acceptance the sale is complete".

2.2.9. Another important feature with regard to validity of consideration under Shariah is that the contract formed has to be free from *'gharar'* and *riba.* The Islamic prohibition against uncertainty requires that the price must be in existence and determined at the time of the contract and cannot be fixed at a later date, nor can it be left subject to determination by a third party. When the consideration consists of a monetary payment (as opposed to payment in kind), the Muslim jurists require that the currency must be in circulation and that its value and species must be determined exactly. [4]

2.2.10.1 It is to be observed that not only must the elements of contracts be lawful; other attributes incidental to these elements must also be lawful. When the payment is made by conventional credit card that is subject to charging of monthly interest, the transaction is void. Here the price is lawful yet the payment is effected in a way that involves the practice of *riba.* Thus, although the consideration by itself is lawful it is still Islamically illegal when the operation of the method of payment is unlawful.

2.2.10.2 Some forms of consideration that may be regarded lawful under the latter are not necessarily so under Islamic contract law principles. Thus things such as pigs and wine cannot be a valid consideration under Islamic contract principles while they are lawful considerations according to the applicable law. Similarly, anything which is useless and/or immoral such as pornographic material is also prohibited by Shariah.

2.2.10.3 These features must be noted and applied by Muslim traders, as being Muslims they are answerable for all their actions in the hereafter and these principles are applicable regardless of whether the commercial affairs are conducted or offered over the Internet.

3. Laws for Electronic Transactions

3.1. United Nations Commission on International Trade Law (UNCITAL) is a core legal body of United Nations with universal membership, specializing in commercial law reform. In order to increase trade worldwide, UNCITRAL is formulating modern, fair, harmonized rules on commercial transactions, including:

> Conventions, model laws and rules that are acceptable worldwide;

> Legal and legislative guides and recommendations of great practical value;

> Updated information on case law and enactments of uniform commercial law;

> Technical assistance in law reform projects; and

> Regional and national seminars on uniform commercial law.

3.2. In the area of electronic transaction and ecommerce, major results of work done at UNCITRAL are.

> Recommendation on the Legal value of Computer Records (1985)

> UNCITRAL Model Law on Electronic Commerce (1996)

4 Rayner, S.E., The Theory of Contract in Islamic Law, at 141

> UNCITRAL Model Law on Electronic Signatures (2001)

3.3. A report was prepared by the UNCITRAL experts on “Legal value of computer records” (A/CN.9/265) and based on that report the Commission adopted the following recommendations to states to review legal requirements:

- Affecting the use of computer records as evidence in litigation;
- That certain trade transactions or trade related documents be in writing;
- necessitate handwritten signature or other paper-based method of authentication on trade related documents; and
- that documents for submission to governments be in writing and manually signed

3.4. The recommendations were endorsed by the General Assembly (Resolution 40/71)

3.5. The Model Law on Electronic Commerce, adopted in 1996 by UNCITRAL, is intended to facilitate the use of modern means of communication and storage of information. It is based on the establishment of a functional equivalent of paper-based concepts such as “writing”, “signature” and “original”. The Model Law also contains rules for electronic commerce in specific areas, such as carriage of goods. With a view to assisting executive branches of Governments, legislative bodies and courts in enacting and interpreting the Model Law, the Commission has also produced a Guide to enactment of the UNCITRAL Model Law on Electronic Commerce. The aim of the Model Law is to provide national legislatures with a template of internationally acceptable rules to remove legal obstacles and thereby create a more secure legal environment for e-commerce. It is intended to facilitate the use of electronic communication by encouraging the international harmonization of domestic legal environments. Over the years the Model Law has gained increasing international acceptance.

3.6. The objectives of the Model Law are to facilitate rather than to regulate electronic commerce; to adapt existing legal requirements and to provide basic legal validity and raise legal certainty. The basic principles of the Model Law are functional equivalence (writing, signature, original), media and technology neutrality and Party autonomy (parties’ choice, choosing level of security).

3.7. The UNCITRAL Model Law on Electronic Signatures, adopted in 2001, is intended to bring additional legal certainty regarding use of electronic signatures. It is built on the flexible principle contained in Article 7 of Model Law on Electronic Commerce. It establishes a presumption that where they meet certain criteria of technical reliability, electronic signatures shall be treated as equivalent to hand-written signatures. This Model Law also follows a technology-neutral approach and avoids favoring the use of any specific technical product.

3.8. The purpose of this Model Law is to encourage international harmonization of laws concerning electronic signatures and certification authorities. It provides conduct rules for various parties dealing with electronic signatures and sets basic standards for the recognition of electronic signatures from other jurisdictions.

3.9. Despite the efforts of UNCITRAL for harmonization of the laws, past few years have seen an explosion of legislative and regulatory work by governments in the field of electronic authentication. The changes in law and advances in technology have dramatically altered the landscape of electronic authentication.

3.10. Legislatures and regulatory agencies around the world have taken various and divergent approaches in their efforts to take advantage of

these emerging technologies. A review of legislative and regulatory activity reveals three basic approaches.

- Minimalist Approach
- Prescriptive Approach
- Two Tier Approach

3.11 Minimalist Approach

3.11.1. Minimalist approach aims to facilitate use of electronic signatures generally, rather than advocate a specific protocol or technology. Traditional common law countries e.g., Canada, US, UK, Australia, and New Zealand, have tended towards minimalist approach.

3.12 Prescriptive Approach

3.12.1. Legislation and regulations enacted under prescriptive approach adopt asymmetric cryptography as the approved means of creating a digital signature; it imposes certain operational and financial requirements on certificate authorities ("CAs"); prescribes duties of key holders; and defines circumstances under which reliance on an electronic signature is justified. Civil law countries have tended to opt for prescriptive approach i.e., Germany, Italy and Argentina but somehow India and Malaysia have also followed this approach.

3.13. Two-tier Approach

3.14. Some jurisdictions have begun to realize that first two approaches are not necessarily mutually exclusive, and so have adopted "two-tier" approach representing convergence and synthesis of the first two approaches. This consolidated approach generally takes the form of enacting laws that prescribe standards for operation of PKIs, and concomitantly take a broad view of what constitutes a valid electronic signature for legal purposes. This "two-tier" approach has found increasing support, most notably in the European Union and Singapore.

4. International Consensus Principles

4.1. International Consensus Principles prepared by Internet law and Policy Forum (ILPF) in Sept' 2000 to create a predictable legal environment are as below:

- Remove legal barriers to electronic authentication;
- Respect freedom of contract and parties' ability to set provisions by agreement;
- Harmonization: make laws governing electronic authentication consistent across jurisdictions;
- Avoid discrimination and erection of non-tariff barriers;
- Allow use of current or future means of electronic authentication; and
- Promote market-driven standards

5. Electronic Transactions Ordinance 2002

5.1. Government of Pakistan adopted its IT Policy in the year 2000 and after studying UNCITRAL model laws, looking at various legislations of both Civil and Common law countries, reviewing different implementation schemes of electronic authentication, regulatory models and best practice guidelines and appreciating the above-mentioned three approaches being followed all over the world, has followed the "International Consensus Principals on Electronic Authentication" designed by Internet Law and Policy Forum and "two-tier" approach.

5.2. The main objective of enacting such law was to move Pakistan from old paper-based transactions to electronic transactions in order to improve its governance, economy and service to citizens in the modern era. At present, barring certain exceptions, all filings/transactions (e.g., tax returns, payments, cheques, banking instructions, custom documents, employment applications, court documents, fee payments, academic transcripts, complaints etc. etc.) are authenticated by signatures on paper, which can then be used as evidence as needed. Electronic transaction, in replacement of or in parallel within this system in vogue, required the backing of law so that the electronic records and digital signatures are acceptable in the eye of law. Electronic Transaction Ordinance 2002 (ETO)[5] was promulgated on September 11, 2002.

5.3. In brief the ETO envisages:

5.3.1 Creation of an Accreditation Council comprising five members appointed by the Federal Government for a period of three years, renewable by another term. The main functions of the council will be to:

- grant and renew accreditation;
- monitor and ensure compliance;
- establish and manage repository;
- carry out research and studies in cryptography services;
- recognize or accredit foreign certification service providers;
- encourage uniformity of standards and practices; and
- make recommendations.

5.3.2. Enabling acceptance of electronic documents/transactions through a certification service provider accredited by the Accredited Council or otherwise, to the court of law;

5.3.3 Giving legal recognition and certain level of presumption to the electronic documents, records, transactions, communication and electronic signatures;

5.3.4 Excusing government and other bodies from accepting electronic filing or effect any monetary transaction in electronic form unless they are ready for it;

5.3.5 Exempting electronic documents, record, communications and transaction from stamp duty for a period of two years so that the provincial governments may be ready to collect stamp duty electronically; and

5.3.6 Making provision of false information, issuance of false certificates, violation of privacy of information and damage to information system crime punishable with imprisonment and fine.

5.4. ETO also provides for appropriate punishments for issuance of false certificates and violations of privacy. The Federal Government may make notifications in the official gazette, make rules to carry out the purposes of this Ordinance, whereas the Accreditation Council may with the prior approval of the Federal Government, make regulations to carry out the purposes of this Ordinance.

6. Sufficiency of ETO

6.1. After promulgation of ETO in 2002, it was realized that in order to be fully ready for e-commerce Pakistan needs to do a bit more than just follow the UNCITRAL Model Law. The other key areas identified requiring legislation are:

- Electronic Banking/Finance
- Data Protection
- Computer related Crimes
- Database Protection
- Employment issues in Information Society
- Liability
- Outsourcing
- Protection of Confidential Information

6.2. From amongst the list, the laws on Data Protection[6], Electronic Crimes[7] and Electronic Banking[8] remained a priority for the Government of Pakistan. Draft bills on these subjects are already being debated and are available on the web for public consultation.

7. Electronic Crimes

7.1 No e-commerce initiative can hold ground or survive unless there is a proper legal system to address the computer related crimes. In case of computer crime or cyber crime, it is more important than ever to legislate so as to prevent unauthorized access to data or information.

7.2.1. Internet users in Pakistan alone are around 8 million. Worldwide, the number of users is estimated to reach 600 million. The economic stakes are also increasing, as e-commerce is expected to reach $ 185 billion and business-to-business e-commerce is projected to reach over $2.7 trillion by the end of this year.

7.2.2. Computers and Internet are connecting people and relaying information. From e-commerce to chat rooms, Internet acts as an extension and facilitator of traditional offline economic and social activities that people have conducted for years before the information age. These activities also include traditional unlawful acts such as fraud and identity theft. Like any technology, computer and Internet are inherently value-neutral tools and can be used by criminals as well as consumers. While some criminal acts such as the recent distributed denial of service (DdoS) attacks on Government websites are unique to the Internet and its technology, most online crimes are “computer version” of offenses with long histories in the real world.

7.2.3. Computers can play three kinds of role in criminal activity. First, computers can be targets of an offense, such as hacking to steal information or attack websites as occurs in denial of service attacks as well as the propagation of computer-viruses. Second, computers can simply be the medium in which an offence is committed: this includes the transmission of pornography, identity theft and fraud. Finally, computers can be incidental to a crime as they may be used to store information or provide other evidence of a crime that has been committed. Computer-related crime poses a serious threat to society; it may target basic utilities, energy, transportation, communication services, military and political institutions. Computer-related crime is becoming increasingly sophisticated; perpetrators more knowledgeable, and increasingly difficult to detect.

---

[6] http://www.pseb.pk/studies/Data%20Protection%20Act-2nd%20V3-rev.pdf
[7] http://www.pakistan.gov.pk/divisions/itandtelecomdivision/media/proposedecrimesact.pdf
[8] http://www.sbp.gov.pk/Isd/PS_EFT_Act_2005.pdf

8. Electronic Crimes Bill

8.1.1. The legislation relating to computer-related crimes is necessitated as the relevant traditional criminal provisions in Pakistan Penal Code and elsewhere exclusively protect physical, tangible and visible objects against traditional crimes. Computer-related crimes not only violate traditional objects in the form of new media but additionally also involve intangible objects e.g. computer programs and date. Traditional legal provisions for damage to property and mischief were developed to protect tangible objects and hence their application to electronic information poses several challenges. The contemporary concept of unauthorized access is sometimes compared to the traditional law concept of trespass but this concept cannot be stretched to protect information stored in computers.

8.1.2. The very nature of these electronic criminal offences brings procedural issues to the forefront of national and international attention as different sovereignties, jurisdictions and laws come into play. More than in any other transnational crime, the speed, mobility and flexibility of computer crime challenge the existing rules of criminal procedural law. Internet has also shown the value of coordinated international action by law enforcement agencies both in exchanging information at the preliminary stage and in preventing the tipping off of other ring members when arrests and seizures are made.

8.1.3. The draftsmen of these laws, it is asserted, while drafting the Electronic Crimes Bill, has examined similar legislations of around 42 countries, Cyber crime Convention of Council of Europe[9] (Commonly known as Budapest Convention) and domestic criminal legislations.

8.1.4. The draft Bill is divided into six Chapters. Chapter 1 contains title, extent, commencement, territorial scope and interpretation clauses. The second Chapter describes offences ranging from simple “access” to “waging cyber war” with appropriate punishments.

8.1.5. The punishments provided in the draft Bill have been taken from the closest offences mentioned in the Pakistan Penal Code and other Pakistani laws. The link between imprisonment and fine is that for every one year a fine of one hundred thousand rupees has been fixed, so if for an offence punishment is three years, fine will be three hundred thousand rupees.

8.1.6. Chapters 3 and 4 deal with powers of investigation and trial of offences. Chapter 5 contains provisions regarding international co-operation, whereas Chapter 6 includes provisions regarding amendment in Electronic Transactions Ordinance and gives this law overriding effect.

9. Child Pornography

9.1.1. This law does not address the crimes related to pornography. The area of child pornography is particularly sensitive as all the developed countries have started a war against such criminals so if child pornography is not a crime in Pakistan, this place will be a haven for predators. Interestingly in the first draft child pornography was a crime but in the latest draft it is missing.

9.1.2. Our children are already victims of all sorts of abuse both at home and outside and if child pornography is not made a crime, we should be ready to see porn pictures and videos of our children floating in the cyberspace.

[9] http://conventions.coe.int/Treaty/En/Treaties/Hum1/185.htm

10. Electronic Data Protection & Constitution

10.1. It is interesting to note the reasons for defining and protecting privacy worldwide. In Central Europe, South America and South Africa privacy protection is provided to remedy past injustices; and Central and eastern European countries are either ensuring that laws are consistent with pan-European laws or adopting laws with hope of joining the EU, whereas in Asia the reason is to promote electronic commerce. The Constitution of Islamic Republic of Pakistan, 1973[10] under Article 14 in the chapter of Fundamental Rights, recognizes right of privacy as a fundamental right:

> **"14. Inviolability of dignity of man, etc.** –
> *(1) The dignity of man and, subject to law, the privacy of home, shall be inviolable.*
>
> *(2) No person shall be subjected to torture for the purpose of extracting evidence.* [11]

10.2. The provision of Article 14 guarantees the dignity of man and subject to law, the privacy of home etc.. [12] Since the right of dignity of man has been guaranteed by the Constitution itself, therefore any law that violates this right will *per se* be unconstitutional.

10.3. Privacy of home is also guaranteed, but this protection is subject to law. Eavesdropping, tapping, stealthily photographing inside the house are invasions of privacy [13] and as such are not permissible under the Constitution as well as in Islam as held by the superior courts in Pakistan while interpreting Article 14. [14]

10.4. In Pakistan the demand for having a law on data protection mainly came from the companies having business outsourced to them from European countries. Although as noted above the Constitution of Pakistan, as well as the Pakistani law on Freedom of Information recognize the right to privacy but the main objective of the draft Pakistani Data Protection Law is not to enshrine the principles of Islam on privacy but to satisfy the requirements of EU Directive 95/46, in particular Article 25 thereof, with the hope of ensuring that data will be allowed to flow freely between the EU and Pakistan, thus making Pakistan an attractive market for outsourcing.

10.5. The usual issues and questions which are considered by non-EU countries at the time of framing and enforcing these laws were:

10.5.1. Is this Law required?
10.5.2. Do we really need this Law?
10.5.3. Should it only be restricted to foreign data?
10.5.4. What are the financial implications of this Law?
10.5.5. What would be the impact on the industry?
10.5.6. Why can't we have the "safe harbor" scheme, if other countries can live with it?

---

[10] http://202.83.164.7/law-division/publications/constitution.pdf
[11] The Constitution of Islamic Republic of Pakistan, Vol. 1. Firs Edition; Commentary by: Emanuel Zaffar. Irfan Law Book House, Lahore
[12] Ghayyur Hussain Shah v Gharib Alam: PLD 1990 Lah 432.
[13] Benazir Bhutto Vs. President of Pakistan PLD 1998 SC 388 (502, 565 & 606)
[14] Manzoor Ahmad v State: 1990 MLD 1488

10.6. These very issues were debated in Pakistan also and after much discussion it was agreed that this law will have positive impact on the economy. Various drafts were prepared: first draft was a very comprehensive legislation following laws of selected EU countries, whereas the second draft was only restricted to foreign data but the latest draft addresses both local and foreign data.

10.7. The latest draft, available on the web, is expected to achieve following objectives:

- Ensure accountability and openness;
- Identify purposes at time of collection;
- Collect information with knowledge and consent;
- Limit use and disclosure;
- Obtain consent for other purposes;
- Ensure that personal data are accurate, complete and up-to date;
- Ensure data security;
- Allow individual access and correction;
- Allow individual redress; and
- Establish oversight responsibility.

10.8. Main features of the draft legislation are:

- Applies to processing of data taking place within Pakistan;
- Facilitates without regulating;
- Respects agreements between parties;
- Complaint of Eighth Principle of EU Directive on Data Protection;
- Exempts Government Data and data for private use;
- Local and Foreign Data treated separately;
- Data Processor to follow instructions of Data Controller;
- Rights of Data Subject only against Data Controller; and
- Data security, minimum measures to be prescribed.

Disclosure only permitted:

- With consent of data controller;
- On Court order;
- Where Law requires; and
- In the interest of national security.

10.9. This law makes following actions, crimes:

- Unlawful processing of electronic data;
- Unlawful dissemination and disclosure; and
- Failure to adopt appropriate data security measures.

10.10. This law also gives protection to whistleblowers.

11. Criticism of Draft Electronic Data Protection Law

11.1. This law was not only reviewed internally but was also published on the web for public comments and interesting comments came from international bodies also. So far the main criticisms of the draft have been that:

- It only applies to private sector and public sector is exempt from its operation;
- Adequate oversight is lacking; and
- Strong language on collection, retention and subject access is required.

12. Electronic Banking & Finance

12.1. After the IT Policy there were many IT initiatives. Meanwhile, the State Bank of Pakistan also allowed opening of the internet merchant accounts and mandatory connectivity to the existing two ATM switches by all the banks to support these initiatives.

12.2. In order to assess the special needs of the banking sector in the cyberspace, some meetings and seminars were held. In these meetings legal issues relating to banks were identified in the areas of:

- Inter-bank payment systems;
- Consumer Electronic Banking;
- Digital Cash;
- Dematerialization;
- Confidentiality and Data Protection; and
- Evidence and security

12.3. There is also a need to have a deeper look into the relations between financial institutions, traders and service establishments and consumers. Regarding transactions by electronic payment instruments, the relationship between car-holder and card issuer also needs to be well defined. To make Internet Banking a reality, the legal principles for regulating financial services on the Internet need to be framed and legal and technological infrastructures for electronic payments system have to be in place. The subject of Digital Cash also, sooner or later, has to be recognized and regulated.

12.4. The legal and practical impact of the dematerialization of shipping documents, electronic bills of lading and its transmission and electronic banking

Documents also have to be assessed. The subject of evidence and security is of vital importance to the banking institutions, especially in relation to document imaging and liability for computer errors in online banking. Confidentiality and Data Protection issues are equally significant.

13. Payments Systems and Electronic Fund Transfer Bill

13.1. The draft prepared by State Bank of Pakistan for e-banking namely the “Payment Systems and Electronic Fund Transfers Bill” is a good attempt but it does not cover all the areas identified above. Moreover it totally ignores the electronic finance and does not encourage micro payment systems.

13.2. The draft bill consists of 10 chapters. The areas covered in this law are

- Payment systems
- Real-time gross settlement
- Payment Instruments
- Electronic Fund Transfer
- Liability of Consumer and financial institution
- Secrecy

14. Amendments in Customs Act 1969

14.1. Through Finance Act, 2003 new sections 30A, 79A, 80A, 81A, 131A, 155A, to 155P were inserted in the Customs Act, 1969 to establish computerized system for Customs and facilitate clearance of goods electronically. The language of these provisions shows that provisions of ETO have been totally ignored.

15. CBR Rules

15.1. CBR issued “Electronic Filing of Sales Tax Return Rules, 2005[15]” and “Electronic Filing of Federal Excise Return Rules, 2005[16]” on December 1, 2005. Both these rules are very sketchy, vendor specific and do not fulfill the requirements of Section 16 of ETO.

16. Next Step

16.1. Overall the situation of cyber laws is very encouraging in Pakistan and we are ahead of many developing countries in this respect. The analysis of the above laws shows that there should be some well-coordinated effort to critically review drafts already prepared and prepare drafts of remaining required laws with single focal point in the Federal Government to avoid conflicts, overlapping and gaps.

---

[15] http://www.cbr.gov.pk/newst/sros/2005/2005/sro1184.htm
[16] http://www.cbr.gov.pk/newce/sros/2005/2005sro1185.htm

Other Cyber Laws Implemented in Pakistan. 1. Prevention of Electronic Crimes Ordinance, 2007 2. Electronic Transactions Ordinance, 2002 3. Pakistan Telecommunication Re-organisation Act, 1996. 4. Wireless Telegraphy Act, 1933 5. Telegraph Act, 1885 6. Federal Investigation Agency Act, 1974. Other initiatives Other initiatives taken by Government of Pakistan include the formation of a National Response Center to stop internet misuse and trace those involved in cyber crimes. The Accreditation Council, in line with the National IT Policy and the Electronic Transactions Ordinance 2002, was also fo See more of Cyber Law Society of Pakistan on Facebook. Log In. or. Create New Account. See more of Cyber Law Society of Pakistan on Facebook. Log In. Forgot account? or. The link contains all information on Cyber Crime Laws in Pakistan.Â The leading Law Firm of Cyber crime cases is Hamza and Hamza Law Associates, who have dealt with numerous Cyber Crime cases lately. With the growth of the internet, wired and wireless networks, web cameras, and the easy availability of information, smart phones, and tablets, opportunities for computer-based crime are growing, and law enforcement is devoting increasing resources to these cases. Commonly referred to as Cyber Crime, these violations involve activity where a computer or network is the source, tool, target, or place of a crime. Also on the rise are false allegations of cyber stalki