How Can we Control Cyber Crime in Pakistan

Abstract

In an effort to gather the basic information related cyber laws and molding that information into the definition for Cyber Environment. Gathering laws implemented in different parts of the world, related Cyber environment, and trying to extract the common factors in those statutes. The measures we need to take to control those factors. Is there any state or authority or body, which is self sufficient in controlling cyber crime? What is the position of Pakistan in their control over cyber crime in Pakistan?

Introduction

World being globalized, due to resource sharing, Strong networks, Social contacts, Moral bindings and of course due to the cyber environment. Cyber environment plays a vital role in supporting all the above mentioned factors. Everything on this earth is bound by some law; either it is natural or manmade. Natural laws are of universal nature. However the manmade laws, are made to avoid any mishap, and of course to cover new technologies and inventions. For example aviation laws are designed to avoid any confusion or mishap in the air traffic. Similarly with the modern advancement and technologies, the laws also need to get modern and more advanced, especially to cover those technologies which become part of public use. Computers and Internet is one of such technology. It has penetrated in our lives so much that life is incomplete without it. There is no comparison of the speed with which people adopted computer culture as compared to the speed of its legislation. No timely measures were taken to fence this technology with proper laws. Due to this, cyber environment got complicated for the nations. Especially in late 90's, things got more devastating. Internet becomes a tool for entertainment for the public, either for pornism or to tease people.

Definition of Cyber Environment

We need to first define this computer created culture i.e. 'Cyber Environment'. Cyber Environment is a self generated term, basically combination of two words i.e. Cyber and environment. It gives the following meaning:

"Our surrounding which involves living things, non-living things and virtual things"

Features of Cyber Environment

Every environment has its own features. These features are subject to the constituents of the environment. Their effectiveness is subject to their minority or majority. One thing very much interesting about cyber environment is that it is of universal nature. There is only one Cyber Environment in the world. We don't have different cyber environments for nations. Even the weather, language, culture, all these things have no effect in the formation of cyber environment. For example the May 2000 LOVE BUG virus whose perpetrator was in Philippines. This virus caused billions of dollars damage to the world. The world realizes it, when the Philippines Government attempted to prosecute the culprit but feel helpless. Mainly because there was no proper legislation to prosecute such person.

For this, we need awareness, knowledge and of course the power to control cyber environment. In fact we need to design mechanism for positive use of this environment. There are no traditions, special laws or any spiritual teachings for cyber environment. One simple rule to follow while drafting law is, respect the privacy of others and don't mingle with things which don't concern you.

Cyber Crime in International Perspective

We might have noticed that there is massive increase in efforts for controlling the free internet space. This change can be very easily pointed out after the September 11 attack on twin towers in USA. A person sitting in any remote area of the world using internet got affected with such measures because he is part of such cyber environment.

According to Reporters Sans Frontiers, 2003 was the "Black year", as China has been declared the world's largest prison for Reporters, cyber dissidents and internet users. Similarly in 2004, Vietnam set up a computer research department mainly to create Internet Surveillance Software.

According to the Electronic Privacy Information Center (EPIC) and Privacy International Report, legislative surveillance is identified in the global trends, which weakened data protection regimes.

Few examples of such harshness are as China Communist authorities start using a variety of tools to discourage free expression on Internet. According to IFEX (International Freedom of Expression Exchange), December 2003, 48 Chinese citizens have been arrested for the offence of free expression. The military Junta in Burma barred all Internet activity by civil society (Lintner, 2001). Singapore restricts civil society internet space by passing a bill in 2001. They draw boundaries on political campaigning over the internet and also barring the publication of opinion polls during general election.

All the above activities, restrictions, measures show one thing in common that after the incident of 9/11 2001, the whole cyber environment was shaken. During this era such devastating changes in the Cyber Environment were notable, irrespective of their geological boundaries or difference of nations.

Cyber Environment in Pakistan

According to an unofficial survey, the software piracy rate in Pakistan is estimated to be about 85%. Important point is, Are those people who are involved in this act are aware that they are committing software piracy. Do they know the meaning of this term? Being a Law student, I can come up with a definition, or may be with the law dealing with such offence but the Law is not for Law students, it is for public and *public needs awareness*.

According to public view, they are not stealing the CD from a shop in fact they are buying it for a reasonable amount from a shop in open market, they pay consideration in form of cash for the contents of the CD. Therefore he is satisfied on moral grounds. Point is we want to correct things without addressing them.

Cyber Laws in Pakistan

Cyber Laws in Pakistan don't have any exceptional history, as seen in the international trend, the cyber law making in Pakistan started mainly after 2001 i.e. Electronic Transaction Ordinance 2002. Furthermore a very pointing law, promulgated in 2007, i.e. Prevention of Electronic Crime Ordinance 2007 (PECO). I happened to study the PECO in reference to some cases. It looks good, complete and comprehensive and covering crime from every angle committed in a cyber environment. In start, I feel good about it but later on one thing keeps bothering me i.e. it did not provide a complete remedy for Intellectual Property rights infringement.

Later on, somehow I came to get a copy of Indian Information Technology Act 2000[1] . Things were very disappointing. I feel a very big and huge unfilled gap in the legislation of PECO, 2007. In fact I personally didn't notice it unless or until I happened to get the Indian act for comparison. This unfilled gap was the awareness. Awareness methods through which one can keep himself safe and secure. Here I am giving a comparison in a table form for the chapters of IT BILL 2000(India), ETO 2002(Pakistan) and PECO 2007(Pakistan).

[1] MGIP(PLU)MRND—1359G1—14-6-2000.

	Name of Chapters		
Law	**IT Bill 2000, India**	**ETO 2002, Pakistan**	**PECO 2007, Pakistan**
1	Preliminary	Preliminary	Preliminary
2	**Digital Signature**	Recognition and Presumption	Offences and Punishments
3	**Electronic Governance**	**Electronic Documents**	Prosecution and Trial of offences
4	**Attribution, Acknowledgment and Despatch of Electronic records**	Certification Service Providers	Establishment of Investigation and Prosecution Agencies
5	**Secure Electronic Records and secure digital Signatures**	Certification Council	International Cooperation
6	**Regulation of Certifying Authority**	Amendments of Certain Laws	Information and Communication Technologies Tribunal
7	**Digital Signature Certificates**	Other Laws and Jurisdictions	Misc
8	Duties of Subscribers	Offences	
9	Penalties and Adjudication	Misc	
10	The Cyber Regulation Appellate		
11	Offences		
12	Network Service Providers not to be liable in certain cases		
13	Misc		

In the above mentioned table, I tried to bring things in a very simple comparison. Nature and the basic architect of the different laws can be easily classified to make some conclusion. If we have a look on the IT bill 2000, which is implemented in India, we will notice that the designer has designed the Law with its basic emphasis on the awareness and introducing safety procedures. Whereas if we have a look to our laws structure, we do find punishments but no procedure to avoid those punishments or to avoid becoming a target or part of any such criminal activity which comes in the domain of cyber environment. Do we find any such thing in our laws?

I appreciate the steps our government has so far taken in establishing grounds for Laws related cyber environment in Pakistan. My request to the government is to change the nature and style of our legislation. May be we can adopt any more better and advanced model of cyber environment then other countries but not more disappointing.

What Measures Should Government take?

An incomplete and criminal nature of legislation supports the law enforcement agencies to misuse the loop holes left in the legislation. Our law should be focused on the procedures one can take to avoid any mishap. It is very unfortunate that in PECO, we don't even find a single chapter related safety precautions. We don't find anything dealing with the procedures for avoiding any cyber crime.

According to my point of view, in today's world, computers are the weapons and therefore if we equip someone with this weapon, it's the duty of government to also give them awareness of this weapon for its positive use. The government should initiate awareness campaign. The main interesting thing in this awareness campaign is that domain of this campaign is well defined i.e. computer literate or technology literate. What I suggest is that the government should introduce a compulsory subject in universities, from where most of our technology related public belongs. Contents of such subject should be covering the cyber environment, how to avoid being a target of cyber crimes or becoming part of such crimes. Such Subject should be from the Government to guide and to educate the computer literates about these cyber crimes. This will result in a network of information and automatically we will see the results of such awareness and control over cyber environment.