**Prevention of Electronic Crimes Ordinance, 2007 an ordinance**

To make provision for prevention of the electronic crimes, 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: -

**Short title, extent application and commencement. -**

* This Ordinance may be called the Prevention of Electronic Crimes Ordinance, 2007.
* It extends to the whole of Pakistan.
* 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.
* It shall come into force at once.

**OFFENCES AND PUNISHMENTS**

**Criminal access**

Whoever intentionally gains unauthorized access to the whole or any part of an electronic system or electronic device with or without infringing security measures, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine not exceeding three hundred thousand rupees, or with both.

**Criminal data access**

Whoever intentionally causes any electronic system or electronic device to perform any function for the purpose of gaining unauthorized access to any data held in any electronic system or electronic device or on obtaining such unauthorized access shall be punished with imprisonment of either description for a term which may extend to three years, or with fine or with both.

**Data damage**

Whoever with intent to illegal gain or cause harm to the public or any person, damages any data is shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both?

**System damage**

Whoever with intent to cause damage to the public or any person interferes with or interrupts or obstructs the functioning, reliability or usefulness of an electronic system or electronic device by inputting, transmitting, damaging, deleting, altering, tempering, deteriorating or suppressing any data or services or halting electronic system or choking the networks shall be punished with imprisonment of either description for a term which may extend to three years, or with fine or, with both.

**Explanation:** For the purpose of this section the expression “services” include any kind of serviceprovided through electronic system.

**Electronic fraud**

Whoever for wrongful gain interferes with or uses any data, electronic system or electronic device or induces any person to enter into a relationship or with intent to deceive any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with Both.

**Electronic forgery**

Whoever for wrongful gain interferes with data, electronic system or electronic device, with intent to cause damage or injury to the public or to any person, or to make any illegal claim or title or to cause any person to part with property or to enter into any express or implied contract, or with intent to commit fraud by any input, alteration, deletion, or suppression of data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine or with both.

**Misuse of electronic system or electronic device**

**a.** Whoever produces, possesses, sells, procures, transports, imports, distributes or otherwise makesavailable an electronic system or electronic device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established under this Ordinance or a password, access code, or similar data by which the whole or any part of an electronic system or electronic device is capable of being accessed or its functionality compromised or reverse engineered with the intent that it be used for the purpose of committing any of the offences established under this Ordinance, is said to commit offence of misuse of electronic system or electronic devices:

**b**. Whoever commits the offence described in sub-section (1) shall be punishable with imprisonment ofeither description for a term which may extend to three years, or with fine, or with both.

**Unauthorized access to code**

Whoever discloses or obtains any password, access as to code, system design or any other means of gaining access to any electronic system or data with intent to obtain wrongful gain, do reverse engineering or cause wrongful loss to any person or for any other unlawful purpose shall be punished with imprisonment of either description for a term which may extend to three years, or with, or with both.

**Misuse of encryption**

Whoever for the purpose of commission of an offence or concealment of incriminating evidence, knowingly and willfully encrypts any incriminating communication or data contained in electronic system relating to that crime or incriminating evidence, commits the offence of misuse of encryption shall be punished with imprisonment of either description for a term which may extend to five years, or with fine, or with both.

**Malicious code**

**a**. Whoever willfully writes, offers, makes available, distributes or transmits malicious code through anelectronic system or electronic device, with intent to cause harm to any electronic system or resulting in the corruption, destruction, alteration, suppression, theft or loss of data commits the offence of malicious code:

**b**. Whoever commits the offence specified in sub-section (1) shall be punished with imprisonment ofeither description for a term which may extend to five years, or with fine or with both.

**Cyber stalking**

Whoever with intent to coerce, intimidates, or harass any person uses computer, computer network, internet, network site, electronic mail or any other similar means of communication to.

* Communicate obscene, vulgar, profane, lewd, lascivious ,or indecent language, picture or image;
* make any suggestion or proposal of an obscene nature;
* threaten any illegal or immoral act;
* take or distribute pictures or photographs of any person
* without his consent or knowledge;
* display or distribute information in a manner that
* substantially increases the risk of harm or violence to any
* Other person commits the offence of cyber stalking.

**b**. Whoever commits the offence specified in sub-section (1) shall be punishable with imprisonment ofeither description for a term which may extend to seven years or with fine not exceeding three hundred thousand rupees, or with both:

**Spamming**

**a**. Whoever transmits harmful, fraudulent, misleading, illegal or unsolicited electronic messages in bulk toany person without the express permission of the recipient, or causes any electronic system to show any such message or involves in falsified online user account registration or falsified domain name registration for commercial purpose commits the offence of spamming.

**b.** Whoever commits the offence of spamming as described in sub-section (1) shall be punishable withfine not exceeding fifty thousand rupees if he commits this offence of spamming for the first time and for every subsequent. Commission of offence of spamming he shall be punished with imprisonment of three months or with fine, or with both.

**Spoofing. -**

**a.** Whoever establishes a website, or sends an electronic message with a counterfeit source intended to bebelieved by the recipient or visitor or its electronic system to be an authentic source with intent to gain unauthorized access or obtain valuable information which later can be used for any unlawful purposes commits the offence of spooling.

**b**. Whoever commits the offence of spooling specified in sub-section

(1) Shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

**Unauthorized interception. -**

**a**. Whoever without lawful authority intercepts by technical means, transmissions of data to, from orwithin an electronic system including electromagnetic emissions from an electronic system carrying such data commits the offence of unauthorized interception?

**b**. Whoever commits the offence of unauthorized interception described in subsection (1) shall bepunished with imprisonment of either description for a term which may extend to five years, or with fine not exceeding five hundred thousand rupees, or with both.

**Cyber terrorism. -**

Any person, group or organization who, with terroristic intent utilizes, accesses or causes to be accessed a computer or computer network or electronic system or electronic device or by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyber terrorism.

**Explanation1:** For the purposes of this section the expression “terroristic intent” means to act with thepurpose to alarm, frighten, disrupt, harm, damage, or carry out an act of violence against any segment of the population, the Government or entity associated therewith.

**Explanation2:** For the purposes of this section the expression “terroristic act” includes, but is not limitedto, -

1. Altering by addition, deletion, or change or attempting to alter information that may result in the imminent injury, sickness, or death to any segment of the population;
2. Transmission or attempted transmission o a harmful program with the purpose of substantially disrupting or disabling any computer network operated by the Government or any public entity;

Aiding the commission of or attempting to aid the commission of an act of violence against the sovereignty of Pakistan, whether or not the commission of such act of violence is actually completed; or stealing or copying, or attempting to steal or copy, or secure classified information or data necessary to manufacture any form of chemical, biological or nuclear weapon, or any other weapon of mass destruction.

**b.** Whoever commits the offence of cyber terrorism and causes death of any person shall be punishablewith death or imprisonment for life, and with line and in any other case he shall be punishable with imprisonment of either description for a term which may extend to ten years, or with fine not less than ten million rupees, or with both.

**Enhanced punishment for offences involving sensitive electronic systems. -**

1. Whoever causes criminal access to any sensitive electronic system in the course of the commission of any of the offences established under this Ordinance shall, in addition to the punishment prescribed for that offence, be punished with imprisonment of either description for a term which may extend to ten years, or with fine not exceeding one million rupees, or with both.
2. For the purposes of any prosecution under this section, it shall be presumed, until contrary is proved, that the accused had the requisite knowledge that it was a sensitive electronic system.

**Of abets, aids or attempts to commits offence**

1. Any person who knowingly and willfully abets the commission of or who aids to commit or does any act preparatory to or in furtherance of the commission of any offence under this Ordinance shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.
2. Any person who attempts to commit an offence under this Ordinance shall be punished for a term which may extend to oneha1f of the longest term of imprisonment provided for that offence. **Explanation:** For aiding or abetting an offence to be committed under this section, it is immaterialwhether the offence has been committed or not.

**Other offences**

Whoever commits any offence, other than those expressly provided under this Ordinance, with the help of computer .electronic system, electronic device or any other electronic mean; shall be punished, in addition to the punishment provided for that offence. with imprisonment of either description for a term which may extend to two years, or with fine not exceeding two hundred thousand rupees, or with both.

**Offences by corporate body**

A corporate body shall be held liable for an offence under this Ordinance if the offence is committed on its instructions or for its benefit.’ The corporate body shall he punished with fine not less than one hundred thousand rupees or the amount involved in the offence whichever is the higher:

**Explanation:** For the purposes of this section corporate body, includes a body of persons incorporatedunder any law such as trust, waqf, an association, a statutory body or a company.

**Information and Communication Technologies Tribunal**

**31. Information and Communication Technologies Tribunal**

1. As soon as possible after the commencement of this Ordinance, the Federal Government shall, by notification in the official Gazette, constitute the Information and Communication Technologies Tribunal whose principal seat shall be at Islamabad.
2. The Tribunal may hold its sittings at such place or places as the Federal Government may decide.
3. The Tribunal shall consist of a chairman and as many members as the Federal Government may determine but not more than seven members.
4. The Chairman may constitute Benches of the Tribunal and unless otherwise directed by him a Bench shall consist of not less than two members. A Bench shall exercise such powers and discharge such functions as may be prescribed. There shall be established at least one Bench in each province.
5. The Federal Government shall appoint the Chairman and members of the Tribunal.

**Saving Tribunal’s proceedings**

No act or proceedings of the Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of the Tribunal.

**Right to legal representation**

The parties in appeal may either appear in person or authorize one or more legal practitioners, and in case of a corporate body any of its officers, to present the case before the Tribunal.

**Appeal to Tribunals**

Any person aggrieved by any of the following orders may, within fifteen days from the date of such order, prefer an appeal to the Tribunal.

**Appeal to High Court**

Any person aggrieved by any decision or order of the Tribunal made under section 40 may prefer second appeal to the respective High Court within thirty days from the date of the decision or order of the Tribunal.

**Revision of Important basic concepts distinguishing characteristics of online journalism**

* Real time
* Shifted time
* Multimedia
* Interactive

**Characteristics of online journalism**

* Hypertextuality
* Interactivity
* Multimodality
* Immediacy

**Characteristics of the Internet**

1. Anonymity
2. Interactivity
3. Beyond geography
4. Online community
5. Lower cost to participate in the public sphere
6. Lower threshold for self-expression of political opinions

**Impact of Internet on Journalism**

1- Traditional media started developing online presence

2- Anyone can be publisher

3- Internet introduced Mass interaction to mass media

4- Impact of internet on News gathering

5- Impact of internet on Access to information and distribution of News

**Flexible Delivery Platforms**

Online news contents included in searchable databases

SMS on cells

Breaking News emails alerts RSS feed

Impact of internet on Process, Production, Storing, retrieval and Presentation of news.

**What is media convergence?**

* Convergence of media occurs when multiple products come together to form one product with the advantages of all of them.
* Media Convergence is gathering and dissemination of news across a multi- media platform.” - Traci Mitchell.
* Media Convergence is the process of combining and presenting of different media (multimedia) into a single delivery system. The Internet is an example of convergence.
* Data and Voice Services - from separate voice and data services to multimedia applications (IP-Telephony, Web Contact Centers)
* Fixed and Mobile Networks and Services - from separate ones to the single infrastructure: CAMEL, VHE, IPv6, IMS
* Public and Corporate Networks – from dedicated networks to open networks.
* Phone, TV and Computer Terminals – from separate devices to combined multimedia terminals
* Broadcasting services-from broadcasting services to Web based TV services: IATV, VoD, WebTV
* For the consumer: more features in less space.
* For media companies: remaining competitive in the struggle for market dominance.
* An ever-wider range of technologies are being converged into single multipurpose devices.

**Text + photos + audio + video + graphics = multimedia.**

Suppose you decided to profile, a brilliant painter/composer. Which medium, or media, would produce the best story? To display his paintings, you’d use photographs. To present his music, you’d use audio recordings. To show him at work — conducting a rock band or painting — you’d use video footage. To explain the meaning and impact of his art, you’d use text. In short, to create the ideal profile, you’d need multimedia, Cross-platform journalism, Media convergence. Whatever you call it, it’s an idea whose time has finally come. Stories once trapped on paper can now be posted online; stories once confined to text and photographs now integrate audio, video and interactivity. Technological innovations are transforming 21st-century journalism. Your job, your newsroom, even the stories you write will soon change dramatically.

**Digital Divide**

The term digital divide refers to the gap between those people with effective access to digital and information technology and those without access to it. It includes the imbalances in physical access to technology, as well as the imbalances in resources and skills needed to effectively participate as a digital citizen. In others words, it’s the unequal access by some members of the society to information and communications technology, and the unequal acquisition of related skills. Groups often discussed in the context of a digital divide include socioeconomic (rich/poor), racial (white/minority), or geographical (urban/rural). The term global digital divide refers to differences in technology access between countries. Many expressions were used to describe the dichotomy of people’s participation or not in the Information Society such as information poor/ rich or have/ have not, but the most widely spread now is the "Digital Divide". Used by most international organizations, this expression has become the reference term. At first, some narrower definitions of the digital divide were focused only on access to computers and Internet but access alone does not bridge the technology gap. As a result, definitions are much wider today. "The term 'digital divide' describes the fact that the world can be divided into people who do and people who don't have access to - and the capability to use - modern information technology, such as the telephone, television, or the Internet. The digital divide exists between those in cities and those in rural areas. It also exists between the educated and the uneducated, between economic classes, and, globally, between the more and less industrially developed nations".

* "The digital divide is the "Differences based on race, gender, geography,
* economic status, and physical ability:
* In access to information, the Internet and other information technologies
* and services
* In skills, it refers to the gap between knowledge, abilities to use internet
* And abilities to use technologies".

There are two different forms of Digital divide, one between countries but also between groups within a country. Bridges organization extensive report puts it in these terms "Real disparities exist in access to and use of information and communications technology (ICT) between countries (the "international digital divide or global digital divide") and between groups within countries (the "domestic digital divide")".

**Checklist for the analysis of Web sites**

1-How navigable is the site?

2- How readable is the information on the site?

3- Is the site aesthetically pleasing?

4-How informative is the site?

5-How long does it take to get the page loaded onto the screen?

6- How does it look on the different browsers and different resolutions? 7- How does it come with Daily Updates and Breaking News?

8- Does it provide any system to enable readers to alert to mistakes and hold us accountable? 9- Does it provide the facility of Feed back?

10- Does it provide the facility to view or read the old versions of news paper?

11- Does it provide the facility of Search the site because the larger sites need a search feature so visitors do not get lost?

**Useful Tips for Effective Web Design**

1. Fast Loading web site
2. Clear Navigation
3. All Resolutions
4. Browser Compatibility
5. Readable and professional looking fonts
6. Minimize the use of
7. Use of white space
8. Check for broken links

**Blogs and Blogging**

A blog is a website in which items are posted on a regular basis and displayed in reverse chronological order. The term blog is a shortened form of weblog or web log. Authoring a blog, maintaining a blog or adding an article to an existing blog is called “blogging”. Individual articles on a blog are called “blog posts,” “posts” or “entries”. A person who posts these entries is called a “blogger”. A blog comprises text, hypertext, images, and links (to other web pages and to video, audio and other files). Blogs use a conversational style of documentation. Often blogs focus on a particular “area of interest. Some blogs discuss personal experiences.’

**Components of Blogs:**

1- Subject or Header:

2- Content or Body:

3- Comments:

4- Time and Date Stamp:

5- Community:

6- Blogroll:

7- RSS feeds:

8- An archive feature for older articles.

9- Blogs also focus on a particular topic such as a corporate vision, politics, religion, sports, or health.