# Dissecting Proposed Cybercrime Legislation: A First Look

# Introduction:

An article published in yesterday's Dawn provided great detail of a cybercrime legislation drafted by Akram Sheikh Associates, commissioned by the government. Below are some initial and immediate concerns that the proposed legislation raises.

# Analysis:

Chapter II - Electronic Documents and Electronic Signatures

**4. Electronic Signature:**
**(4) The Cyber Authority may add or omit any electronic signature and the procedure for affixing such signature.**

How and why are electronic signatures being tampered with? Why is this the domain of the authority in the first place? This is an individual-to-individual procedure and the Authority's intervention in this process would be a violation of privacy.

CHAPTER III- ATTRIBUTION OF ELECTRONIC DOCUMENTS

**18. Attribution of electronic documents:**
**(1) Unless otherwise agreed as between an originator and the addressee, an electronic document shall be deemed to be that of the originator if it was sent;**
**(b) by a person who had the authority to act on behalf of the originator in respect of that electronic document; or**

This cannot be done, unless you are sharing the authorization code for your digital signature. For instance even if I have access to a computer that has adobe x installed with your digital signatures in it, the private key stored on your computer is encrypted. Any user including yourself, will have to add a password to unlock the private key and use your signatures. This doesn't work like a power of attorney for someone to act on your behalf. In a non-tech world this means you are giving someone permission to forge your signature (or that's how it reads).

CHAPTER IV - CYBER AUTHORITY:

**21.Establishment of Cyber Authority**
**(3) The Cyber Authority of Pakistan shall comprise of seven members, with five members from the private sector and two members from the public sector. One of the members shall be designated as the Chairman by the Federal Government.**

The process by which the members shall be nominated, elected/selected is not mentioned. The term 'private sector' does not indicate whether it pertains only to corporates, whether it includes civil society members etc. There is no governing document with functions, powers and duties clearly defined.

**(4) The Chairman and members of the Cyber Authority shall be appointed by the Federal Government for a term of three years and shall be eligible for reappointment only once for an equal term after**

**the expiry of their first term of appointment.**

If the committee comprises members from both the public and private sectors, why is decision-making solely the federal government's prerogative? Doesn't that pave way for political appointments vs those on merit? Also, what is the eligibility criteria?

**21. Establishment of the Cyber Authority:**
**(8) Once appointed, no member shall have any direct financial or other interest in any entity or business relating to any services to which the Cyber Authority is authorized to function or perform.**

Assuming that the members will likely be domain experts in the field, isn't there a high chance these domain experts will still be intimately related to the field (in either a business, firm etc.) ? It would make sense to state instead that members shall not draw undue benefit/financial benefit from their acting role as a member.

**22. Qualifications of members:**
**(1) Of the seven members of the Cyber Authority:**
**(a) four shall be professionals or academics with at least seven years work experience in the fields of information technology, internet services, telecommunications and cryptography services; (b) two shall be advocates with at least seven years experience and adequate knowledge of laws relating to information technology, internet services, telecommunications and cryptography services; (c) one shall have an administrative background with at least seven years experience in a private or public organization.**

There seems to be a criteria on the face of it but how will the process pan out? Essentially, all members remain appointees as they are selected vs being elected or making it to the committee through an open and transparent process. In its current form, seven-member committee is not accountable to any public forum

**(6) The Cyber Authority may, from time to time, delegate one or more of its functions and powers to one or more of its members.**

This suggests there is no clear division of power, this will be done so at the whims of the Cyber Authority itself.

**(7) A member of the Cyber Authority shall not be removed except on the grounds of misconduct or incapacity as adjudicated by a court of competent jurisdiction.**

This suggests there is no internal code of conduct defined for the authority, any issues, even misconduct will have to be challenged in court.

**(9) Decisions of the Cyber Authority shall be taken by a majority of the members, however the Chairman shall have a casting vote in case of a tie.**

Any act that is prescribed by the Committee must seek input from various stakeholders of the government, industry, civil society, etc. as in seeking a larger forum to be present and see a vote on it (like a general body meeting). No directives or instructions should be passed without an adequate debate and publishing for comments period (typically 45 days).

**23. Functions of Cyber Authority**
**(2) Without prejudice to the generality of the foregoing, the Cyber Authority shall:**
**(a) ensure that cybercrimes, as provided under this Act and otherwise, are effectively prevented, suppressed, investigated and prosecuted;**

How are cybercrimes going to be prevented in the absence of any privacy laws mandated for corporates i.e banks and others or enhanced security measures for private and public companies handling data? Additionally, the proposed legislation does not lay down investigation and prosecution procedures. Leaving these open-ended or at the discretion of Authority once it comes into existence is a glaring loophole, allowing for excessive procedures.

**d) organize a Cyber Prosecution Team composed of members of the Cyber Authority and other persons, as may be designated by the Cyber Authority, to exclusively prosecute persons involved in violations of this Act and other matters connected thereto;**

If the Prosecution Team is being created exclusively, what happens to NR3C under the FIA Act? Does this legislation abolish their mandate - to whatever extent is exists currently? Which 'other persons' are to be involved in the investigation and prosecution process, and what are their roles, responsibilities and limits? None of this is clearly defined.

**(g) cooperate and coordinate with domestic and international persons, entities and agencies in relation to prevention, suppression, investigation or prosecution of cyber-crimes and to fulfill other purposes of this Act and the matters connected thereto;**
**h) facilitate international cooperation on intelligence, investigations, training and capacity building in order to prevent, suppress, investigate and prosecute cybercrimes as provided under this Act and other matters connected thereto;**
**(i) monitor cybercrime cases as prevented and suppressed by cooperating and participating domestic and international law-enforcement agencies;**

Who decides the scope of what or who is engageable ? Shouldn't there be a structured system of authorization ? We would not want the Cyber Authority to arbitrarily form relationships with any/all bodies.

Clauses (g) and (h) both discuss the 'prevention' of cyber-crimes and co-operation with international agencies, without mention of whether data gathered on suspicion will be shared with international intelligence agencies. This is effectively Pakistan's 5 eyes where they are seeking authority to share data or seek international assistance on basis of suspicion for the purpose of 'prevention of crime.' However, what are the confines within which data gathering and sharing is to take place?

**(k) collect or record by electronic means traffic data in real-time associated with specified electronic documents transmitted by means of electronic devices;**

Isn't this paramount to arbitrary data interception (much like the NSA) ? Under what circumstances should this even be permissible? Shouldn't the equivalent of a warrant be required to put this in place first? The manner in which this is phrased suggests that any data transmitted electronically is fair game for surveillance.
Methods of data collection and storage and undefined.

**26. Powers of the Cyber Investigation Team:**

**(1) Subject to the regulations prescribed by the Cyber Authority, the Investigation Team shall be entitled to:**
**(a) access and inspect the operation of any electronic device and any data or program residing therein;**
**(b) access and inspect any information, code, program, technology and other tangible and non-tangible materials;**

The ambit within which the Cyber Investigation Team is to operate should have been a part of the proposed legislation, rather than the Authority laying out the regulations. CIT here is authorized to inspect any electronic device and data in it. Including 'code'. There is no mention on how this process works and warrant issued. The scope or context of the electronic device has not been defined leaving room for abuse. This must indicate clearly through a documented process that any electronic device that the Cyber Investigation Team draws a consensus on is relevant to the investigation at hand, and that this is subject to the approval of a higher authority.

Cyber Authority should not be able to confiscate devices such as computers / cell-phones / tablets etc. without a court-approved warrant at least. Secondly, the Authority should not be allowed to confiscate peripheral computer equipment owned by say family members or office staff, etc.

**(c) require any person to explain or clarify any matter related to any electronic device whether in his ownership, control or otherwise;**

Anyone in possession of a USB seems to be fair game. How and why should investigation be allowed based entirely on possession of an electronic device.

**29. Grant of Accreditation:**
**(1) The Cyber Authority may grant accreditation to certification service provider, its cryptography services, electronic signature and security procedures to any person who complies with the criteria and requirements specified in the regulations prescribed by the Cyber Authority.**
**(2) The terms and conditions of the accreditation, including those relating to duration of the accreditation, renewal, suspension, revocation, fee for grant and renewal, shall be specified in regulations prescribed by the Cyber Authority.**

What precisely constitutes compliance w.r.t. criteria and requirements? The Cyber Authority should not take any steps to establish itself as the Proxy and / or Man in the Middle gatekeeper or checker for any sort of information that traverses between a user and a service outside or inside of Pakistan, this is especially true for Skype, VPN and HTTPS services (to mention at the very least).

Many services like say Google, etc. automatically enable encryption by virtue of HTTPS, by utilizing such a service and such an encryption, an average person should not be subject to cryptography clauses and be subjugated unnecessarily.

**32. Establishment of Cyber Authority Fund**:
**(2) The Fund shall consist of:**
**(b) loans, aid, grants and donations from the national or international agencies;**

Will taking funds from 'international agencies' not expose the authority to the risks of lobbying, influence and loss

in objectivity?

CHAPTER VI- CYBERCRIMES AND PUNISHMENTS

**43. Punishment for committing crimes against Pakistan:**
**(1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in imminent and real danger to any interests of Pakistan including, but not limited to, national security, national economy or public order, shall be punishable with imprisonment of a term not exceeding seven years, or with fine which may extend to ten million rupees, or with both.**

Calling something 'the interest of Pakistan' and then using it as the basis for punishment is high risk and open to abuse. This needs to be better defined. There is no distinction for willful intent, malicious intent or any language that would enforce that determining intent is important. Seven years is a an incredibly harsh punishment for vaguely defined offence.

Also, instead of making this an additional offence, it could very well be classified as an umbrella offence (if it needs to be an offence, in the first place). A person may be charged with an offence apart from Section 43 and if acquitted of that offence, can still be convicted under Section 43 as vaguely defined offences allow arbitrary authority to the executive.

**44. Punishment for damage to electronic device:**

This section in its entirety ranges from punishing hackers to punishing individuals that may end up deleting data on an electronic device.

**45. Punishment for hacking:**
**(1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in hacking of or otherwise gaining unauthorized access into any electronic device, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both.**

Punishment for hacking is too harsh, there is also no understanding of hacktivism or whistleblowing. There are no protections whatsoever and White Hat hacking is not mentioned or even considered.
The offence refers to either performing or causing to perform a function which may result in "hacking" but does not refer to the intent of the accused, whether it was done with intention, recklessness or negligence. These three facets are extremely important in criminal law as the nature of the crime and the sentence levied must reflect the existing mental state of the accused. As the above stated offences have been classified as, "crimes" and not offences falling under Tort (Tort offences only constitute compensation), for the legal conviction of n accused, the mens rea (the mental element) of the crime must be determined with the three elements being either recklessness, intention or negligence. Without the successful determination of the presence of one of these elements within the prosecution and a conviction is allowed, that would constitute a gross miscarriage of justice.

**47. Punishment for dishonestly receiving electronic device:**

**(1) Any person who dishonestly receives or retains any stolen electronic device or any information or data therein knowing or having reason to believe the same to be received or retained dishonestly, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both.**

Dishonestly is vague term. How is this to be determined?

**48. Punishment for identity theft:**
**(1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in fraudulent or dishonest use of an electronic signature, password or any other unique identification feature of any other person, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both.**

**49. Punishment for personation:**
**(1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in personating any other person or otherwise pretending to be any other person, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both.**

Firstly, there is no term such as 'personation.' Impersonation is generally considered Tort and does not fall within the ambit of criminal law. Therefore, it should not be included under criminal offences, nor should it be punishable with imprisonment.

Identity theft, depending on the degree of damage is punishable by jail time. However, this is entirely dependant on the determination of the degree of damage.

**50. Punishment for violation of privacy:**
**(1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in violating any other person's privacy, in any manner whatsoever, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both.**

What constitutes privacy and its violation? There is room for exploitation here. This should be applied on entities, especially those that host data of individuals and not just individuals. However, this needs to be defined, as in what causes privacy breach. Is posting a picture of me by someone else on Facebook without my permission considered a privacy breach that may result in three years in prison? Does this also imply that uploading images on Instagram from my father's iPad, applying filters and significantly altering the existing images, would constitute as image tampering and a breach of privacy for which I can be charged with an offence?

**52. Punishment for cyber terrorism:**
**(1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in threatening the national security of Pakistan, striking terror in any person, destruction of property or committing any other crime termed as terrorist act, shall be punishable with imprisonment of a term not exceeding**

**seven years or fine not exceeding one million rupees, or both.**

"Striking terror in any person" is much too vague. Who decides whether something constitutes a terrorism case or not? How does ATC play in (if at all?). There are very serious charges associated with vague terminology.

**53. Punishment for cyber stalking, spamming, spoofing and squatting:**
**(1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in harassment, intimidation, or coercion, shall commit the crime of cyber stalking.**

**(2) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in transmission of fraudulent, misleading, or unsolicited electronic messages in bulk or otherwise to any person without his express permission, shall commit the offence of cyber spamming.**

Spamming is criminalized whereas it need not be. There are spam filters etc that can adequately deal with this.
**(3) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in sending of electronic messages with a counterfeit source, depicting to be an authentic source, so as to gain unauthorized access or obtain valuable information in an unlawful manner, shall commit the crime of cyber spoofing.**

Spoofing is also done by means of a phishing scam, where the originator is unaware, in that case how is it logical to make it a punishable offence.

**(4) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in acquisition of a domain name in bad faith to mislead, defame and deprive others from registering the same, shall commit the crime of cybersquatting.**

Cybersquatting is when people buy domains or popular domains for the sole reason of reselling them. Cybersquatting again is generally a Tort and should not be criminalized.

**(5) Any person who commits the offence of cyber stalking, spamming, spoofing or squatting as described in sub-sections (1), (2), (3) or (4) respectively shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both.**

Cyber stalking, spamming, spoofing and squatting are not clearly defined.

**54: Punishment for transmitting offensive messages:**
**(1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in sending, generating, publishing or transmitting any information that is offensive, obscene or false in any manner whatsoever and sent for the purpose of causing annoyance, inconvenience, intimidation, hatred, deception, insult, obstruction or injury, shall be punishable with imprisonment of a term not**

**exceeding three years or fine not exceeding five hundred thousand rupees, or both.**

What constitutes offensive? This is a very subjective domain which is being criminalized.

**57. Punishment for transmitting material containing heinous acts:**
**(1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in sending, generating, publishing or transmitting any material which contains any act or conduct that may be considered heinous, odious and atrocious, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both.**

What is considered heinous, odious and atrocious. Who decides this? And how is the mode of transmission determined?

**58. Punishment for failure to protect data:**
**(1) Any person who is responsible for possessing, dealing or handling any sensitive personal data in an electronic device which it owns, controls or operates, and negligent in implementing and maintaining security practices and procedures, thereby causing wrongful loss or gain to any person, shall be liable to pay compensation to the person so affected.**

Negligence in handling data is fairly common, through our experience with digital security training of individuals – from school students to private sector individuals – very few people have an understanding of how to protect their data. In the absence of a privacy policy or any awareness campaigns supported by the federation, punishment of such kinds is overbroad.

Does this imply that if I do not have a security passcode on my cell phone and someone accesses my phone and extracts personal contact information, I can be held liable for failing to secure access to my phone? This clause also infringes upon the personal liberty of an individual. The state cannot impose liability on a mere personal omission.

There is no mention of 'establishing intent.' No mention of responsibility of the owner to take necessary precautions. There is nothing about prevention in this clause. This could easily mean that anyone found to have made an innocent mistake can be charged.

**64. "Offences to be non-bailable, compoundable and cognizable: (1) All offences under this Act shall be non-bailable, compoundable and cognizable"**

Non-bailable means that the court may not permit bail or bail may not be granted; it would be at discretion of court whether to consider a bail application and grant bail. This forces an accused to remain in prison during the course of the trial. Under the act, all the offences are "compoundable" which means that court resolution is not necessary and the parties involved in the dispute can settle things amongst themselves. For example, if you steal from a store, and the owner catches you but instead of taking you to court tells you to compensate by working five days in the shop, that would be settlement of the dispute and courts need not intervene even though you are guilty by law. A cognizable offence is one where the police does not require a warrant to arrest.

For all the above offenses to be non-bailable seems extreme. For terrorism, child sex offenders or other critical circumstances, one can understand for it to be non-bailable, but non-bailable for spam is extreme.

By not requiring an arrest warrant, there are no limits set for the investigating authorities. Neither are they required to provide concrete evidence prior to arrest. In cases of cyber crime. concrete evidence should be of utmost importance as there is a high probability that an innocent can be wrongfully charged. Faisal Chohan's case, which was one of mistaken identity under PECO, is one that proves how easy it is to make a mistake, especially within cybercrime space, and how having a warrant is an absolute necessity.

Overall, the proportionality of punishments for listed offences is questionable.

CHAPTER VIII- REPEAL AND SAVINGS

**74. Application of Act No. XVII of 1996: (1) Notwithstanding anything contained in the Pakistan Telecommunication (Re- organisation) Act, 1996 (XVII of 1996), the Cyber Authority shall be exclusively responsible for the functions described this Act and rules made hereunder.**
**Provided that, the foregoing provision shall not affect the applicability or operation of the provisions of the Pakistan Telecommunication (Reorganisation) Act, 1996 (XVII of 1996) to the telecommunication systems or telecommunication services, other than cryptography services, provided by the cryptography service providers.**

**75. Amendment of Act XVII of 1996: (1) In the Pakistan Telecommunication (Re-organisation) Act, 1996 (XVII of 1996), clause (b) of sub-section (2) of section 57 shall be omitted.**
**(2) Any provision in any license issued by the Pakistan Telecommunication Authority under the aforesaid Act prohibiting the provision or use of cryptography services shall cease to have effect subject to provisions of this Act.**

This Act aims to amend the PTA Act of 1996, so that all cryptography services are amassed under its sole authority.

**76. Repeal of Act LI of 2002: (1) The Electronic Transactions Ordinance 2002 (LI of 2002) shall stand repealed by virtue of this Act, hereinafter referred to as the repealed Ordinance, except the following is saved:**
**(a) The Schedule made under Section 29 of the repealed Ordinance titled as Amendments in Qanun-e-Shahadat Order, 1984 (P.O. No. 10 of 1984).**

ETO is essentially the only legislation applicable in the digital space. ETO pertains to business transactions in particular. Clubbing business transactions within the sphere of crimes and criminal offences is not a wise move. These should remain separate.

## Summary Of Comments

- There is little or no understanding of certificate accreditation and how the system works
- In the case of foreign certificate providers, the government should automatically classify all root authorities to be registered automatically - the government of Pakistan should not expect them to come to Pakistan and comply with our laws
- Private Keys can at no point in time be kept by the Cyber Authority or anyone
- Any corporation or public body that handles data is given a clean chit – there is no mention of any laws that may be applicable to them
- There is still no mention of what occurs if it is the government or an official committing these crimes
- What happens if the Cyber Authority deems as these laws being exploited by members of the public or the government
- The authority and its functions are poorly defined, prone to abuse
- Overall the powers of the authority are neither transparent nor accountable
- Net neutrality is not considered or even understood throughout the course of the document
- The Federation should be moving towards decentralizing control over the Internet, not aspiring to create an NSA-like model
- None of the monitoring and surveillance clauses include 'lawful communication interception through means of a court order'
- The offences listed need to be defined specifically; the terms used are vague and can be abused
- For offences listed that derive their definition from the Cybercrime Bill (currently being considered) this should be specified, definitions should be mentioned
- Proportionality of punishments vs offences listed needs to be revisited
- The mens rea needed to establish crime, is ill structured and vaguely defined with the offences. This leaves room for loopholes and manipulation.
- The need to clearly define mens rea, the procedures to establish it, along with appropriate court proceedings, remain
- The system for recourse for any of the issues are not clearly defined
- Right to appeal should be facilitated by protections; fair chance of hearing needs to be provided before charge is established
- The Act, in its entirety, has missed considerations and right to privacy of citizens; there is no mention of constitutional protections and right to privacy
- Privacy of citizens and data protection should be at the centre of the cybersecurity agenda

## Conclusion:

The proposed legislation does not reflect a clear understanding of digital space or medium, and lacks adequate safeguards that should be in place to curb violations and excesses which have been committed in the past, under the Prevention of Electronic Crimes Ordinance, which is what led to its redrafting.

Other than the vague definitions, what this proposed legislation misses is description and detail of processes by which a crime is to be determined. In the electronic and digital medium, the process that leads to an action is of utmost importance. Determination of the crime is directly linked to that. Failure to establish a chain of deliberate and intentional events that lead to an action undermine the strength of the case. And so, with the processes and methods of determination undefined, the legislation remains open-ended and liable to misuse. This could potentially cause innocents to be charged and tried - a concern that has been highlighted in the past.

This brings us to the proportionality of punishments as well as the method of investigation and trial. Firstly, it is questionable whether some offences listed in this legislation should be considered offences in the first place. Many of them, elsewhere, are considered as Tort. Secondly, the authorities constituted and the functions and powers ascribed appear to be too wide-ranging.

The manner of their constitution, appointment, functioning and decision-making is centralised, with the controls in the hands of the federal government. The little representation of private entities for which provision is created is also left to the discretion of government authorities, allowing them to handpick candidates. The authorities are created with the goal of empowering them to be the law unto themselves, instead of creating a system of checks and balances. Instead of devolving authority so as to require warrants, and establish a clear method of investigation and trial that should include a documented procedure that is to be followed, no boundaries have been ascribed to the authorities.

There is no consideration of the event that if the said authorities were to overstep their mandate - which in fact is not clearly defined - how is that event to be dealt with. While there are punishments for citizens, nothing is prescribed for authorities and officials when they commit a mistake or deliberately misuse authority.

Most disturbing are some of functions which are unheard of, and can only undermine the security and integrity of information systems in the country. To this extent, certification accreditation and cryptography are of great concern.

It is quite startling to see that various portions of this proposed legislation have been replicated in their entirety from the Information Technology Act of 2000 of India. For example: Section 44 is a copy of Section 43 of the IT Act 2000 of India, Section 45 is a copy of Section 66 of the IT Act, and Section 54 and 55 are mere offshoots of Section 67 of the IT Act of 2000. It would be unwise to consider the Information technology Act of 2000 as a stepping stone, as the Act was heavily criticized for infringing upon personal liberties of Indian citizens. Moreover, it did not take into consideration evolving technologies and new forms of communication which is why in 2008, the Information

Technology Act of 2000 was heavily amended by the Indian Parliament and the Amended IT Act of 2008 was introduced.

Similarly, the Prevention of Electronic Crimes Ordinance, when first proposed received heavy criticism from civil advocacy and industry groups due to the degree to which it ignored civil liberties, business continuity and a sheer disregard of international practices. The legislation aimed to instill upon the citizens a harsh brand of justice which was evidence of not a democratic and aware society but more of a police state. This ultimately led to its redrafting.

Any proposed legislation should ensure it is not violative of due process and fundamental rights considerations. These should be at the very centre of lawmaking. The uncanny resemblance of the proposed legislation under discussion in this paper, to the discarded Indian IT Act and PECO indicates that little or no attention was paid to the concerns raised previously.

The approach to lawmaking in the digital space, as we have seen repeatedly, is undertaken with little or no knowledge of the nature of digital mediums and devices. It is futile to draw from existing frameworks and replicate those for electronic/digital media. Unless very specific, practical, implementable aspects of the functioning of these mediums is taken into consideration, laws will continue to remain irrelevant, unsound and repressive. Sound technical knowledge along with clear standards of rights and privacy are the very first requirement for law-making in this space. This expertise, as we have seen in the past, remains missing within the policy-making circles. Multi-stakeholder input is the only way forward. And we expect that when the time to table legislation arrives, the multistakeholder approach is the one adopted over political expediency.