The Prevention of Electronic Crimes Bill 2015

Process:

The biggest failing has been the process – or lack of – as far as the drafting of the Prevention of Electronic Crimes Bill 2015 is concerned. It has taken place behind closed doors, with the exclusion of members of opposition, and without any public or expert input.

Despite repeated attempts by members of opposition, industry and civil society groups to provide input and make this a public and transparent process, all such efforts have been thwarted. Repeated requests for meetings and hearings have been denied. Meetings, to which members of opposition were invited, have been scheduled at a day's notice at times.

Despite all the verbal and written input provided, next to nothing has been accommodated in the latest approved version of the bill. Not only was the bill once again approved with much haste, but a copy of the bill was not even placed before the members of the NA Standing Committee on IT to review before casting a vote.

Content:

The proposed bill will function as a **gag law** should it come to pass in its current form. It prescribes blanket censorship, curtails political speech, and seeks to control dissenting views, debate and dialogue, sanctioned particularly under **Section 34**. This section is a copy paste of Article 19 of the Constitution and the Pakistan Telecommunications Authority (PTA) is directly empowered to interpret the exclusion clauses and remove content from the Internet or any information system as it deems fit.

Much is left to the **discretion** of authorized officers, authorities and agencies, and the federal government. **Overbroad powers** have been given to regulatory and investigation bodies without any checks and balances or accountability mechanisms. For instance, Section 32 gives an authorized officer the power to ask someone to divulge encryption keys or passwords. This forces an individual - and by default those connected to him her – to divulge and provide access to private data beyond what may be necessary or within the scope of the investigation. It also poses a risk to companies who are required to sign confidentiality agreements or MoUs for business.

Judicial oversight, with the exception of requiring warrants for search and seizure, remains absent in the proposed law. Data and information are everything today. Authorities and officers should not get easy access to it unless legitimately required and as sanctioned by court.

The proposed bill does not distinguish between innocent people and criminals. In turn, it prescribes heavy penalties in the form of jail terms and fines. Whistle-blowers, white-hat hackers etc also run the risk of being treated as common criminals.

Loosely worded sections leave too much room for interpretation and misinterpretation, widening the window for **misuse** and likelihood of the provisions of this bill being used for score-settling rather than addressing criminal activity.

Recommendations:

The bill needs to be heavily **amended** to bring it line with a constitutional framework that **safeguards rights**. This should be done through an open, transparent and consultative process. Citizens' right to privacy, speech and due process need to be ensured.

Speech-related offences and those that pertain to the telecom sector should be omitted from this bill; only computer/medium specific crimes should remain.

The **age** distinguishing a minor and an adult should be 18.

'**Malicious intent**' should be added to all sections on offences to establish mens rea.

Warrants should be required for not only search and seizure, but for all offences. An officer should have to provide reasoning before court as to why access to a person's data, device or to the accused himself/herself is necessary. This becomes all the more necessary in the absence of data protection and privacy legislation.

Procedures should be defined under this law rather than left up to the rule-making powers of the government. Moreover, the rule-making powers of the government should also be subjected to public scrutiny – all proposed rules should go through the public eye before coming into effect.

Penalties should exist for service providers and investigation officers who step beyond the scope of duty and misuse information they may gain access to – especially in the absence of privacy and data protection legislation.

Cooperation with foreign governments and entities – and on what terms – should be subjected to a well-defined procedure stipulated under this law. The data of Pakistani citizens should not be readily shared or handed over - protections and procedures need to be in place. Again, especially since data protection and privacy laws do not exist.

Conclusion:

Given that there is still relatively low computer and technology literacy in the country, a law that deals with crimes needs to be carefully crafted. While it should serve the rightful purpose of curtailing criminal activity, it should not place the fear of technology among a people still embracing and learning to use this medium. Neither should it treat every user as a potential criminal. The bill, in its current form, is likely to inculcate the fear of technology, which would negatively impact the growth the ICT sector has witnessed or the manner in which people have embraced technology - for the good.