Major Concerns: Prevention of Electronic Crimes Bill

Curbs on Speech, Expression and Access to Information

18: Natural Dignity of a Person – criminalizes the act of exhibiting, displaying or transmitting 'false information,' which is 'likely' to 'harm or intimidate the reputation or privacy of a natural person.' While this doesn't apply to anything aired on television, it applies to everything uploaded and shared online. Political expression and satire is not exempted. Some examples how this can be misapplied:

The person who uploaded Rehman Malik's video of boarding a flight late would be jailed for it. In fact he did lose his job and was charged under the Maintenance of Public Order. PTI activist Qazi Jalal was charged under Section 36 & 37 of the ETO for a tweet in which he alleged a judge's son-in-law was deriving benefits due to his in-laws' position. He included a wedding card in his tweet to corroborate the person in question was actually the son-in-law. In Turkey, a man is facing a two-year jail term for sharing a meme comparing Erdogan and Gollum – character from the Lord Of The Rings Trilogy. Would the same happen to person who created/shared the Nawaz Sharif & Shrek meme? And any other form of political expression, satire or citizen journalism will be construed as harm to reputation. Either people will start to self-censor – as is now rampant on channels and do a great degree in print – or people will be facing jail terms.

21: Cyber Stalking – The following acts are criminalized under this section: (a) 'communicate obscene, vulgar, contemptuous and indecent information;' (b) 'any suggestion or proposal of an obscene nature;' (c) threaten to commit any illegal or immoral act; (d) take a picture of any person and display or distribute without his consent or knowledge in a manner that harms the person.

Whose definition of 'obscene, vulgar, contemptuous, indecent, obscene and immoral' would be applied? What about pictures taken without permission if they are covering crowds at public events? Or those pictures zeroing in on public/known figures attending rallies/congregations by banned organizations, in an attempt to call them out or hold them accountable for it? This carries a jail term of up to three years.

34: Powers to manage on-line information – The PTA is given policing powers: 'empowered to manage information and issue directions for removal or blocking of access of any information through any information system.' Moreover 'the Authority may direct any service provider to remove any information or block access to such information if it considers it necessary' as per the exceptions listed out in Article 19.

This clause gives the government/PTA unfettered powers to block access or remove speech not only on the Internet but transmitted through any device. It is a copy-paste of Article 19, allowing the PTA to interpret how the exclusions are to be applied. Just like PEMRA issues directives to the electronic television channels, PTA would do the same to ISPs.

In the past, Beyghairat Bridage's video critical of the army was blocked. Shia killings, a website that documents sectarian killings, stands blocked. IMDB, a movie database was blocked because there was a review and link to a documentary on Balochistan on it. Instagram was blocked on the pretext of there being pornographic material available on it.

All the alternate views found on the Mina tragedy that emerged on social media would stand blocked. No dissenting view would be available on Balochistan. As it is, several sites stand blocked on the pretext of them being 'anti-state.' Any commentary on religion or a view other one particular sect's interpretation could be blocked in the name of protecting 'the glory of Islam.' The Internet in Pakistan will become an extended version of PTV: all dissenting views would be controlled and only the state version.

……

In all three sections mentioned above, PTA is given sole discretion over content. In the case of Sections 18 and 21, while they are non-cognizable and compoundable, the 'aggrieved' can apply directly to PTA for 'removal or destruction of, or blocking access of such information' and 'the Authority may on receipt of such application may take such measures as deemed appropriate fir removal or destruction of, or blocking access to, such information.' In Section 34, no one has to apply to PTA; it can act unilaterally and issue instructions as it deems fit.

Privacy

28. Expedited preservation and acquisition of data – An 'authorized officer' may write to a person in control of an information system and require him/her to provide data or order that specified data be preserved up to 90 days. It is after this is done that the authorized officer must bring this to the court's attention within 24 hours. So post-PECB, we will be receiving written orders from not even the agency but an officer, to hand over data. 24 hours is long enough a period to misuse the powers given.

29: Retention of data – a service provider (i.e. ISP) is required to retain data (of its customers) up to a year and provide it to the investigation agency or authorized officer as and when notified by the Authority to do so. Our entire digital footprint – what we accessed, who we communicated with and the specific contents – would be on offer.

32: Powers of an authorized officer Sub-section (g) requires the disclosure of encryption keys (passwords etc), forces an individual 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. The 'authorized officer' is empowered to make this request/notify person without seeking court approval.

33: Dealing with seized data - Currently this has been left to the discretion of the federal government and its rule-making powers, while the procedure should clearly be stipulated under this bill (as it was in the stakeholder version). What would happen to an information system or device once it is seized? Who will ensure the information and data in the device or system is not browsed through – or damaged/altered/deleted. While for investigation purposes, a specific file may be required, however the ability to access other files would also exist once the device is in possession. One person's device/information system also provides access to thousands of other people, who fall well beyond the scope of investigation.

36. Real-time collection and recording of information – Based on an application by an authorized officer, 'if a Court is satisfied that the content or any information is reasonably required for the purposed of a specific criminal investigation, the court may order with respect to information held by or passing through a service provider, to a designated agency…having the capability to collect real time information, to collect or record such information in coordination with the investigation agency.' For a period of seven days, real-time activity will be recorded as sanctioned by court. Everything as it is being typed and transmitted would be recorded and visible. There is no mention of the capability and methods that will be used to do this – how invasive they would be. The same instruments used to record for seven days can (and most likely will) be used for continued and selective and/or broad-based surveillance.

……

While in the revised version of the bill Section 31: Warrant for content data, has been added, whether or not it would apply to the above sections and how, is ambiguous. Section 31 reads: 'upon the application by an authorized officer that demonstrates to the satisfaction of the court that there exist reasonable grounds to believe that the content data stored in an information system is reasonably required…the Court may, after recording reasons, order that a person in control of the information system or data, to provide such data or access to the authorized officer.'

Section 31 pertains to the 'disclosure of content data.' It speaks nothing of data other than content data. In this bill, data is defined as 'traffic data and content data.' Moreover other forms of 'data' are covered under other definitions. Information for instance is defined as: 'text, message, data, voice, sound, database, video, signals, software, computer programs, any form of intelligence as defined under the PTA (Reorganization Act 1996 and codes including object code and source code.'

So while a warrant would be required for disclosure of 'content data,' there is no procedure nor oversight prescribed for the acquisition, disclosure, retention, preservation or handling of traffic data – which is also identifiable data (i.e. can reveal a person's location and identity. Nor does this exist for information – the definition for which contains nearly all forms of data. Moreover Section 31 deals with a person in control of the information system or data, and not service providers or those storing data on behalf of others. Therefore the token warrant for content data hardly serves as a safeguard for the above-listed sections, which give sweeping powers over - and intrusive access - to everyone's communication and data. And there is no data protection or privacy legislation in Pakistan.