Pakistan: New Cybercrime Bill Threatens the Rights to Privacy and Free Expression

ARTICLE 19 and Digital Rights Foundation Pakistan have serious concerns about measures contained in Pakistan's proposed *Prevention of Electronic Crimes* Bill ('PEC Bill'). The Bill contains a number of provisions that, if implemented, would violate the rights to freedom of expression and privacy. We urge members of the Senate of Pakistan to reject the Bill and call on the Pakistani parliament to ensure that any new cybercrime legislation is fully compliant with international human rights standards.

Our concerns

In ARTICLE 19 and Digital Rights Foundation Pakistan's view, the PEC Bill violates international standards on freedom of expression for the following reasons:

1. **Power to manage intelligence and issue directions for removal or blocking of access of any intelligence through any information system:** we are concerned by section 34 of the Bill, which grants new sweeping powers to the Pakistan Telecommunications Authority ('PTA') to "manage intelligence" and order the removal or blocking of access to "any" information online without a determination of its legality by a court. In particular, the PTA or 'any officer authorised by it on its behalf', may direct any service provider to remove any intelligence or block access to such intelligence if it considers it necessary 'in the interests of the glory of Islam' or the 'integrity, security or defence of Pakistan' or on the grounds of 'friendly relations with foreign states, public order, decency, morality, contempt of court, commission of or incitement to an offence. In other words, this section grants *carte blanche* to the government to restrict access to any information on the Internet it dislikes. The grounds on which access to such information may be restricted go far beyond the legitimate aims exhaustively listed under Article 19 of the International Covenant on Civil and Political Rights. This includes for instance the 'glory of Islam', 'friendly relations with foreign states' and 'decency'. Moreover, and any event, the section entirely fails to provide for a right of appeal or judicial review of the decisions of the PTA. Instead, section 34 (2) merely provides that the Federal Government 'may prescribe rules for adoption of standards and procedure by the Authority to monitor and block access and entertain complaints under this section'.

We are further concerned that section 34 (2) and (3) give the Government broad powers to use technology, such as deep packet inspection, to monitor online content in breach of international standards on freedom of expression and privacy. In this regard, the four special mandates on freedom of expression have held in their 2011 Joint Declaration on Freedom of Expression that "content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression".

In short, section 34 is overly broad and fails to include adequate safeguards for the protection of the rights to freedom of expression and privacy in breach of international human rights law.

Recommendation:

- Section 34 should be rejected in its entirety.

2. **Overbroad offences against misuse of computers and lack of public interest defence:** in our analysis of an earlier draft of the Bill, we had noted that offences against misuse of computers or 'hacking' types offences failed to provide for a public interest defences for cases where unauthorised access to information systems, programmes or data may take place for legitimate purposes, such as investigative journalism or research. These concerns remain unaddressed.

   Instead, the vast majority of the previous offences against misuse of computers have been replaced by a smaller number of provisions drafted in overly broad language and with fewer safeguards. For instance, section 3 of the Bill criminalises "whoever intentionally gains unauthorised access to any information system or data". The offence is punishable by imprisonment for a term, which may extend to 3 months or a fine of up to 50,000 rupees or both. This offence is hopelessly broad, in violation of the legality requirement under international human rights law. If the Bill were adopted, individuals seeking access to information on websites blocked by the government could potentially be prosecuted, as access to that information would not be 'authorised'. Furthermore, the section 3-offence falls well below the best practice standards set by the Cybercrime Convention 2001. In particular, the offence fails to include a requirement that the offence be committed by infringing security measures and/or 'intent of obtaining computer data or other dishonest intent.

   Similar concerns apply to section 5 of the Bill, which introduces the offence of interference with information system or data without requiring that such interference result in serious harm. In the absence of such requirement or a public interest defence, the Bill fails to recognise that interest groups may legitimately engage in peaceful 'online protest' by seeking to disrupt access to a website without causing any real damage to that site. This would be the case, for instance, if traffic to a government webpage were temporarily redirected to an interstitial webpage containing a lawful message.

   Even more disturbingly, section 4 of the Bill criminalises the unauthorised copying or transmission of data. Whilst the offence includes a requirement of 'intent', as currently drafted, we are concerned that Internet Service Providers could be prosecuted for transmitting data if they are not authorised to do so. In other words,

the provision seemingly introduces some wholly undefined licensing requirement. We also note that the Cybercrime Convention does not include any requirement for States to adopt any provisions of this kind. In our view, it is much too broad and in breach of the legality requirement under international human rights law.

Recommendation:

- Sections 3-5 should be revised and at a minimum be brought more closely in line with the requirements of the Cybercrime Convention.
- A public interest defence should be introduced for 'hacking'-type of offences.

3. **Glorification of an offence and hate speech**: the PEC Bill introduces a new offence of "glorification of an offence and hate speech" under section 9. In our view, this offence is drafted in overly broad terms in breach of international standards on freedom of expression. In particular, the criminalisation of the 'glorification of an offence or the person accused or convicted of a crime' under section 9 (a) would stifle debate on what the law should or should not criminalise as well as the application of the criminal law in individual cases. Furthermore, the previous UN Special rapporteur on Freedom of Expression, Frank La Rue, made it clear in his May 2011 report that the term 'glorification' fails to meet the requirement of legality under international human rights law. The same is equally true of terms such as "support" of terrorism, which are wholly unclear.

   Recommendation*:*

   - Section 9 should be removed in its entirety.
   - To the extent that the Pakistani government may wish to prohibit incitement to discrimination, hostility or violence or incitement to terrorism, it should do so consistently with the requirements of international standards on freedom of expression. In this regard, we note that the four special mandates have held in their 2008 Joint Declaration on defamation of religions, and anti-terrorism, and anti-extremism legislation that:

     "The criminalisation of speech relating to terrorism should be restricted to instances of intentional incitement to terrorism, understood as a direct call to engage in terrorism which is directly responsible for increasing the likelihood of a terrorist act occurring, or to actual participation in terrorist acts (for example by directing them). Vague notions such as providing communications support to terrorism or extremism, the 'glorification' or 'promotion' of terrorism or extremism, and the mere repetition of statements by terrorists, which does not itself constitute incitement, should not be criminalised."

4. **Overly broad cyber-terrorism offence:** the cyber-terrorism offence remains drafted in excessively-broad language. The concerns we highlighted in our March 2014 statement remain unaddressed. Cyber-terrorism offences must be much more clearly linked to violence and the risk of harm and injury in the real world and in particular harm against the welfare of the individuals. In particular, any coercion or intimidation must be directed at individuals and create a sense of fear or panic in the public or section of the public rather than the Government as currently provided is section 10 (a). In this regard, we draw attention to the model definition of terrorism proposed by

the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has proposed the following model definition of terrorism:

"Terrorism means an action or attempted action where:

1. *The action:*
   (a) Constituted the intentional taking of hostages; or
   (b) Is intended to cause death or serious bodily injury to one or more members of the general population or segments of it; or
   (c) Involved lethal or serious physical violence against one or more members of the general population or segments of it;

   AND

2. *The action is done or attempted with the intention of:*
   (a) Provoking a state of terror in the general public or segment of it; or
   (b) Compelling a Government of international organisation to do or abstain from doing something

   AND

3. *The action corresponds to:*
   (a) The definition of a serious offence in national law, enacted for the purpose of complying with international conventions and protocols relating to terrorism or with resolutions of the Security Council relating to terrorism; or
   (b) All elements of a serious crime defined by national law." (A/HRC/51, para. 28). "

Recommendation:

- Section 10 should be revised in light of the above concerns and brought more closely in line with the model definition of terrorism outline above.

5. **Offences against dignity of natural persons:** an earlier attempt to criminalise defamation against women has been considerably broadened to criminalise offences against the dignity of natural persons under section 18 of the new PEC Bill. Section 18 (1) punishes with criminal sanctions "whoever intentionally publicly exhibits or displays or transmits any false intelligence, which is likely to harm or intimidate the reputation or privacy of a natural person". Leaving aside that reputation or privacy cannot be 'intimidated', this provision effectively criminalises defamation in breach of international standards on freedom of expression. In its General Comment no. 34 the UN Human Rights Committee stated that States parties should consider the decriminalisation of defamation and that criminal law should only be applied in the most *serious* cases. Moreover, even where defamation is a civil wrong, the law should provide that a statement is not defamatory unless its publication has caused or is likely to cause serious harm to the reputation of the claimant.

   Equally, we take the view that the publication of private information in breach of confidence or the misuse of private information should be treated as civil wrongs rather than criminal offences as is the case under the PEC Bill. We are further

concerned that section 18 (2) provides for a new remedy that would allow aggrieved persons to apply for injunctions ordering the removal, destruction or blocking of access to material in breach of section 18 (1). Although attempts at protecting the right to privacy and reputation are legitimate, we believe that these types of injunctions are ineffective at achieving their stated purpose due to the nature of the Internet itself. In particular, in the case of blocking measures, there is a real risk that access to legitimate information may be restricted due to well-known attendant risks of overblocking or underblocking.

Recommendation:

- Section 18 should be removed.

6. **Offences against modesty or a natural person and minor:** section 19 of the PEC Bill introduces a new offence against the modesty of a natural person or minor. In particular, section 19 (1) criminalises "whoever intentionally and publicly exhibits, displays or transmits any intelligence which (a) superimposes a photograph of the face of a natural person over any sexually explicit image; or (b) distorts the face of a natural person or the inclusion of a photograph or a video of a natural person in a sexually explicit conduct; or (c) intimidates a natural person with any sexual act".

   Again, while attempts to protect the dignity of natural persons are laudable, and with the exception of section 19 (c), we question whether the criminal law is the most effective way of dealing with these types of behaviour. This is especially so in the absence of a requirement to prove serious harm to the victim. Furthermore, and in any event, allowance should be made for the fact that sexually explicit images may be used for journalistic purposes, e.g. to report on the character of politicians or public officials. Equally, superimposing someone's image over a sexually explicit image may be used as a form of humour, e.g. in caricatures to distil a political message (see, *mutatis mutandis*, Palomo Sanchez v Spain, ECtHR, 12 September 2011).

   Recommendation:

   - Section 19 should be removed or at least revised in light of the above concerns.

7. **Cyberstalking**: Section 21 criminalises the use of the Internet or other information systems etc. to: (a) communicate "obscene, vulgar, contemptuous, or indecent intelligence", or (b) "to make any suggestion or proposal of an obscene nature; or (c) threaten to commit any illegal or immoral act; or (d) take a picture or photograph of any person and display or distribute without his concern or consent or knowledge in a manner that harms the person; or "display or distribute information in a manner that substantially increases the risk of harm or violence to any person", with intent to coerce, intimidate or harass any person. While the inclusion of a *means rea* requirement - namely intent to coerce, intimidate or harass any person – is positive, we are concerned that individuals could be prosecuted by reference to content, which remains entirely undefined. In particular, the terms 'obscene', 'vulgar', 'contemptuous' are not given any definition. Nor could they, as these terms are inherently vague.

Equally, section 21 fails to make allowance for the fact that photographs may be taken and used without the consent or knowledge of a person for journalistic purposes. While a public figure may feel that the use of such photograph may be a form of intimidation or harassment, it would be perfectly legitimate in the context of reporting on the character of such figure.

More generally, we question the need for specific offences in this area. In our view, it would be better to deal with the underlying mischief in such cases by way of general provisions against harassment, stalking, intimidation and threats of harm under the Criminal Code.

Recommendation:

- Section 21 should be removed or at least substantially revised. In particular, section 21 (1) (a) to (e) and section 21 (3) should be struck out.

8. **Spoofing:** section 23 introduces a new offence of spoofing. While this section is presumably aimed at dealing with counterfeiting websites, we are concerned that it fails to provide safeguards against its potential misuse against individuals setting up humorous websites mocking well-known brands. As such, this offence is overly broad and risks having a serious chilling effect on the right to freedom of expression. We also note that spoofing seemingly criminalises a different type of conduct in other countries, such as the United States where it is used in criminal proceedings involving a form of market manipulation.

   Recommendation:

   - Section 23 should be removed.

9. **Criminalising the production, distribution and use of encryption tools:** we are concerned that sections 13 and 16 may be used to criminalise the production, distribution and use of encryption tools enabling anonymity online. Section 13 criminalises whoever produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device intending or believing it primarily to be used to commit or to assist in the commission of an offence under this Act. In our view, this provision could be used to crack down on software programmers who produce goods that may be used for both legitimate and illegitimate purposes. In particular, programmes such as Tor enable users to be anonymous online. The Bill makes no distinction between a tiny proportion of users who might use anonymity for criminal purposes and the vast majority of legitimate users of such anonymity tools who simply wish to protect their right to privacy whilst reading or sharing information online. Given the borderless nature of the Internet and the differences between the types of cyber-offences from country to country, it would be impossible to establish whether a programmer knew or intended the programme to be used for the commission of an offence. In any event, it would constitute a disproportionate restriction on the exercise of freedom of expression and the right to privacy.

   Section 16 further criminalises whoever unlawfully or without authorisation changes, alters, tampers with or re-programmes unique device identifiers of any communication

equipment and starts using or marketing such device for transmitting and receiving 'intelligence'. We are concerned that this provision might be used to crackdown on manufacturers, suppliers and users of programmes such as Tor or proxy servers that enable anonymous browsing online. In our view, this is a disproportionate restriction on the exercise of the right to freedom of expression as well as the right to read and browse anonymously online.

Recommendation:

- Both section 13 and 16 should be removed.

Pakistan's cybercrime bill must be open to public scrutiny

In addition to concerns over many of the measures contained in the Bill, the parliamentary procedure adopted by the National Assembly has been gravely flawed. In particular, a previous draft of the Bill that was made public in March 2014 appears to have been entirely redrafted behind closed doors by a group convened by the National Assembly Standing Committee. Not only does the new draft ignore criticisms of the earlier draft but introduces a number of fresh provisions that would violate the rights to freedom of expression and privacy under international law. By excluding civil society and the private sector from consultation on the Bill, the government has prevented genuine public scrutiny of the Bill prior to the vote in the National Assembly and – in doing so – has undermined the democratic process in Pakistan.