Analysis of Pakistan's cyber-crime bill

by Reporters Without Borders (RSF) and Freedom Network

The National Assembly Standing Committee on Information Technology and Telecommunication approved the latest draft of the Prevention of Electronic Act Crimes 2015 on 16 April.

Although Reporters Without Borders (RSF) recognises the need for governments to draft legislation that takes account of the spread of the Internet and to protect Internet users from cyber-crime, any legislation must comply with international human rights standards and in particular with the obligation to respect freedom of expression and information. More specifically, in June 2010 Pakistan ratified the International Covenant on Civil and Political Rights (ICCPR), article 19 (3) of which requires that any restrictions on the right to freedom of expression must satisfy a three-part test, according to the interpretation provided by the UN Human Rights Committee in its General Comment No. 34.

This latest version of the cyber-crime bill constitutes a serious threat to the fundamental rights to privacy and freedom of expression of Pakistani citizens, as well as to the work and safety of journalists in Pakistan. Several of the bill's provisions violate fundamental rights and international standards on freedom of expression, and pose a serious threat to the ability of journalists to work freely.

Section 3 and 4 on unauthorized access to information systems and on copying and transmitting information systems or data

- Too broad wording
Section 3 and 4 of the bill criminalize the intentional access to "*any*" information system or data, and the intentional copying and transmission of "*any*" data, when unauthorized. This very broad wording criminalizes accessing, copying and transmitting *any* information system or data, whether critical, secret, restricted, classified, private, copyrighted, personal or open to the public.

These sections should be rendered more precise and their scope narrowed so that:

- only unauthorized access to "critical" or "restricted" information systems or data is forbidden
- only unauthorized copying of copyrighted or critical data is forbidden
- only unauthorized transmission of data that could harm the rights or reputation of others or that would threaten national security, public order, public health or morality is forbidden, in accordance with article 19 (3) of the ICCPR.

Moreover, the bill should be amended so that

- only the unauthorized accessing, copying or transmission of information systems or data *committed with the intent to cause harm or loss or obtain an illegitimate advantage* is criminalized.

- Serious threat to the free exercise of journalism
Although it is legitimate to protect information systems from unauthorized access, sections 3 and 4 of the bill pose a serious threat to the ability of journalists to work freely, especially investigative journalists, whose work consists precisely in accessing information they are not authorized to access. Offences as defined in section 3 and 4 of the bill could therefore have a strong chilling effect on media activities in Pakistan.
Similarly, the law as currently drafted could seriously impact revelations by whistleblowers, who by definition reveal information of general interest by transmitting data they are not authorized to access, copy or transmit.

The bill should therefore make an exception for journalists and news providers, who should never be prosecuted for accessing information systems or data without authorization.

- Criminalizing innocuous behaviour
It must also be noted that not only journalists but also the average Internet user could be gravely impacted by these provisions. Since section 2 (d) of the bill defines "unauthorized access" as "access without authorization *or in violation of the terms and conditions of the authorization,*" any person accessing or visiting a website in a way that that is not expressly authorized is committing a crime. In practice, this means that anyone who in any way breaches a website's terms of use (not reading terms of use is very common) or who just copies and pastes a single sentence from a webpage without express authorization could end up in jail for up to six months.

- **Disproportionate penalties**

The penalties stipulated in sections 3 and 4 (respectively, three months in prison and/or a fine of 50,000 rupees, and six months in prison and/or a fine 100,000 rupees) are disproportionate, especially for such innocuous behaviours as those described above, and should therefore be drastically reduced.

Section 9 on glorifying an offence and hate speech

- Too broad wording

Section 9 of the bill on "glorification of an offence and hate speech" criminalizes not only the glorification of terrorism or proscribed organizations, which is authorized by international law, but also criminalizes anyone who "prepares or disseminates" (or even threatens to do so) any type of information that would glorify a person "accused of a crime" or that would "advance religious, ethnic or sectarian hatred (...) through any information system or device."

The lack of definition and precision about the offences named in section 9 could result in overly broad and abusive interpretation. It could lead, for example, to the arrest and prosecution of anyone who blogged about a person being prosecuted, or even lawyers who defend their clients on the Internet.

Moreover, anyone who *threatens* to glorify a person "accused of a crime" or to "advance religious, ethnic or sectarian hatred" could also be prosecuted. Not only the free expression of such discourse but also the mere threat of it is proscribed, which restricts freedom of expression even further.

- Serious threat to the work of journalists and news providers

Section 9 therefore not only violates the fundamental principle of presumption of innocence and the right to freedom of expression but also poses a serious threat to the ability of journalists to work freely. Journalists could face prosecution for expressing a legitimate opinion about a person who has been arrested or for writing an article that could be seen as insufficiently critical of terrorism, religious hatred or other kinds of hatred. This could results in a major increase in self-censorship by journalists fearing prosecution in connection with their reporting or the views they express.

Moreover, nowhere does the bill indicate how glorification of an offence is evaluated, what criteria are to be used or what level of criticism is necessary to avoid the "glorification" label. As currently worded, the bill defines what journalists may report and what views they may express. For example, it would forbid them to ever express positive views about an accused person. This violates freedom of opinion and expression, and violates Pakistan's international obligations.

Section 10 on "cyber-terrorism"

- Too broad wording

Section 10 defines cyber-terrorism as committing or threatening to commit an "unauthorized access to critical infrastructure information system," "unauthorized copying or transmission to critical infrastructure data," "interference with critical infrastructure

information system or data", and "glorification of an offence and hate speech" when there is an intent to create a sense of fear or insecurity in the government or the public or to advance religious, ethnic, or sectarian discord.

The lack of definition is troublesome. How is a "sense of insecurity in the government" to be defined? Would any of these acts, if committed without authorization, be defined as terrorism if they made the government feel insecure? Couldn't any of these acts be defined as terrorism if the motive was political?

- Serious threat to the work of journalists and news providers
This very vague and broad wording poses a serious threat to the work of journalists and whistleblowers, who could be prosecuted on a cyber-terrorism charge if they revealed information the government chose to define as critical. Section 2 (j) of the bill says that "critical infrastructure includes any other infrastructure so designated by the Government." The authorities could designate an infrastructure as critical so that anyone transmitting information or data about it could be prosecuted as a terrorist if they were not authorized to access it.

- **Disproportionate penalties**
Section 10 sets very severe penalties (14 years of imprisonment and/or a fine up to 15 million rupees) when offences defined under sections 6 to 9 are committed for the purpose of terrorism. It sets the same severe penalties in cases of a threat to commit these acts. Such long prison terms are not acceptable for the mere threat of committing an act, and should be drastically reduced.

Section 10 also specifies the same penalties for glorification of an accused person with the intent to create a sense of fear or insecurity in the government or the public or to advance religious, ethnic or sectarian discord. Such severe penalties for expressing an opinion are disproportionate and should be reduced.

Section 18 on offences against a person's dignity

Section 18 criminalizes transmitting "false intelligence" likely to harm or threaten a person's reputation or privacy.

- Too broad wording
Although the protection of reputation and privacy is legitimate, the wording of section 18 is unclear.

Private individuals have a right to protect their reputation or privacy whether the intelligence is true or false. International standards permit restrictions on freedom of expression if they are necessary for the "respect of the rights or reputations of others" (article 19 of the ICCPR) regardless of the veracity of the information transmitted. The reference to "*false intelligence*" has the effect of reducing the individual's rights. Transmitting accurate information about an individual via the Internet would not be liable to prosecution even when it violated their privacy or harmed their reputation. The bill says nothing about the possibility for the person prosecuted to prove the accuracy of the information or about the

need for the subject of the information to demonstrate any threat to their privacy or reputation.

- Serious threat to the activities of journalists and news providers
The use of the word "*likely*"(in "*false intelligence which is likely to harm the reputation…*") suggests that it is false information that is targeted, and not violations of reputation or privacy, which are only potential. This provision poses a serious danger to the work of journalists, who could find themselves being prosecuted for transmitting erroneous or partially inaccurate information that could, for example, affect a politician's reputation. Journalists have an obligation to check the information they report but not to guarantee its accuracy. The possibility of such prosecutions would increase self-censorship and limit revelations by investigative journalists, and would therefore constitute a grave violation of freedom of information.

The bill should make an exception for journalists, who must never be prosecuted for transmitting erroneous information. Under international law, only a deliberate attack on a person's reputation, rights or privacy can be prosecuted.

- Excessive powers over media activities
The person affected by "*false information*" can turn to the Pakistan Telecommunication Authority to obtain the withdrawal, destruction of blocking of access to this information without the intervention of a judge. A government agency could therefore order a media outlet to remove an article containing "*false information*" without any established procedure for determining whether the information was false. Giving the authorities such excessive power over the media opens the way to censorship. It therefore constitutes a grave danger to the work of journalists and a serious violation of freedom of the media and information.

The bill should stipulate that only a judge may order the withdrawal, suppression or blocking of information if it constitutes an attack on the plaintiff's reputation or rights, and that the judge may issue such an order only after a hearing at which the person who disseminated this information is able to defend their actions.

- **Disproportionate penalties**
The penalties established in section 18 for the transmission of false information (three years in prison and/or a fine of 1 million rupees) are out of all proportion in the case of a journalist who reports erroneous information. Journalists must never be imprisoned for the information they report, whether accurate or erroneous.

Section 19 on offences against modesty of persons/minors

- Lack of definition and too broad wording
Section 19 penalizes certain actions of a sexual nature, above with the aim of protecting minors. It also makes it a crime to "distort the face of a natural person." In the absence of a definition of this crime, it could include the playful distortion of the photo of a face, as made possible by a number of widely distributed and widely used software applications. Such innocent and harmless behaviour should not be subject to such a severe penalty as seven years in prison.

The bill should specify that such behaviour is forbidden if it is carried out with the intent of causing harm or obtaining an undue advantage.

- Serious threat to the ability of journalists to work

In the absence of a definition of the crime of "distorting a face," one can also envisage its application to pixelating a face to make it anonymous or even turning a face into a caricature. This provision therefore constitutes a serious threat to the confidentiality of journalists' sources, who would no longer dare to speak on camera, and therefore to media freedom.

Section 22 on spamming

Section 22 defines spamming as the transmission of "harmful, fraudulent, misleading, illegal or unsolicited intelligence to any person without the express permission of the recipient." The reference to "unsolicited" would make it an offence to send an email, photo or a text message or post a photo or a comment on a social network without the recipient's express and prior permission. As this would pose a serious problem for the free flow of communication in Pakistan, this section should be amended to delete the reference to "unsolicited."

Section 28 on expedited preservation and acquisition of data

- Excessive powers

Section 28 would allow an "*authorized officer*" to require any person controlling an *information system* to provide or keep any data that are "*reasonably necessary*" to his investigation, without the intervention or authorization of a judge. No warrant would be necessary and the officer would simply have to inform the court, which would not verify the grounds for the request, the need for the information or the proportionality between the request and the investigation's needs.

The relationship between section 28 and sections 30 and 31 regarding court orders is unclear. If section 28 is subject to the provisions of sections 30 and 31, especially as regards the need for the authorized officer to obtain an order from a judge in order to exercise his power, this must be stated.

- Serious threat to the work of journalists

These excessive powers constitute a grave violation of the right to privacy and the confidentiality of journalists' sources. Journalists would not longer be certain that they would be able to keep information confidential if the authorities just had to claim that they needed the information for an investigation in order to obtain it. And no source would be able to trust a journalist.

Section 29 on retention of traffic data

Section 29 would oblige all Internet Service Providers to retain all Internet traffic data for a year and to provide the data to the authorities whenever they so requested.

- Excessive surveillance powers

Section 28 increases state surveillance powers considerably. The bill's previous draft required the retention of data traffic for 90 days. The extension of this period is a disturbing sign. An obligation to retain data for a year is excessive. As the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression said in his report of 3 May 2013, "National data retention laws are invasive and costly, and threaten the rights to privacy and free expression. (...) Mandatory data retention laws greatly increase the scope of State surveillance, and thus the scope for infringements upon human rights."

Moreover, as already stated, allowing the authorities to demand the surrender of data without any intervention or control by a judge constitutes a grave attack on the right to privacy and the confidentiality of sources. The Pakistani state's power to keep its population under surveillance would be excessive.

- Chilling effect on freedom of expression

The mere fact that all communications are recorded has a chilling effect on freedom of expression. International law regards the privacy and anonymity of communications as legitimate and as a legal right. They are also necessary for the work of journalists and their sources as well as for whistleblowers. As the Special Rapporteur for the right to freedom of expression said in his 2013 report, mass Internet surveillance violates human rights and has a negative impact on journalists.

Aside from the fact that this provision seriously violates email confidentiality, privacy and the confidentiality of sources, the data that has been gathered, compiled and stored becomes vulnerable to theft or privacy, a danger that is increased by the length of the data retention period.

Section 32 on the powers of authorized officers

- Excessive powers

As currently drafted, section 32 gives a number of powers to "authorized officers" without any apparent provision for the intervention of a judge and without any obligation to request or obtain a warrant or order before these powers are exercised. These powers are therefore excessive. Section 32 allows an authorized officer "to have access to (...) any information system," "to search any information system," to demand the keys needed to

decrypt files, and to require any person to provide access to an information system if there is “reasonable cause” to believe that it has been used by that person or has been used on the person’s behalf. These powers are excessive and intrusive, and constitute a definite threat to the privacy of Pakistani citizens.

The relationship between section 32 and sections 30 and 31 regarding court orders is unclear. If section 32 is subject to the provisions of sections 30 and 31, especially as regards the need for the authorized officer to obtain an order from a judge in order to exercise the power listed in section 32, this must be stated. If the provisions of sections 30 and 31 do not apply, section 32 must be amended so that the powers of authorized officers can only be exercised under a judge’s control. A warrant seems to be needed in order to “search,” “seize” or “disclose” data but not to obtain access to an information system or a decryption key.

- Serious threat to the work of journalists

These powers are excessive and constitute a threat to the work of journalists and the confidentiality of their sources. If the authorities can demand access to a journalist’s email account or the key to encrypted information, journalists and their informants will no longer be able to be certain that their communications will remain confidential.

Even if procedural guarantees were attached to the use of the powers defined in the current draft, an exception should be made for journalists and the confidentiality of their sources, so that their data may be collected, inspected, seized or decrypted only on a judge’s order, only in the event of a threat to national security or grave danger to the physical safety or a person or persons, only if this information is essential in order to prevent the realization of this threat or danger, and only if the information cannot be obtained in any other manner.

Section 34 on the power to control information

Section 34 is one of the bill’s most problematic sections and constitutes a disturbing evolution in the bill compared with previous drafts. It would allow the government to “*issue directions (to service providers) for removal or blocking of access of any intelligence through any information system* (...) *if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign states, public order, decency or morality or in relation to contempt of court or commission of or incitement to an offence under this Act.*”

- Unconstitutionality

This section 34, which mentions the article 19 of the Constitution is problematic : using certain parts of any constitutional provision in any other statutory law without its specific context is against the spirit of the Constitution. It is therefore unconstitutional to leave this to a statutory body like PTA or its authorized officer to decide about the fundamental right of citizens and block or remove any information from any website. Any government authority, including PTA, must not have any role in contents management by blocking a website or anything else. A broad-based representative

civil society body with adequate authority/power should be mandated to do contents audit.

- Broad censorship power
This section would give the authorities the power to censor any online content or prevent access to it without any control by a court.

In the absence of a definition of the "*interest of the glory of Islam*" and information as to how it is evaluated (especially as it is questionable whether authorized officers are best placed to evaluate it), in the absence of a definition of decency and morality and information as to how they are evaluated, and given the vague and excessively broad grounds for withdrawing or blocking information, section 34 gives the authorities the power to censor any website or any information passing through the Internet that they regard as inappropriate or disturbing.

Any information on a sensitive subject, any discussion on a forum and any photo posted on a social network could be censored or blocked on the grounds that it posed a threat to Islam, decency or Pakistan's security.

These censorship powers constitute a complete violation of freedom of expression and Pakistan's international obligations.

- Lack of procedural safeguards
Section 34 does not provide for reference to a judge prior to censorship, does not provide for any form of appeal, whether to a government agency or to a court, and does not even provide for the possibility of an appeal against the censorship after the event. These powers would open the way to abuses and would constitute a major setback for civil liberties.

- Serious threat to free speech and the work of journalists
Section 34 poses a grave threat to freedom of expression in Pakistan and to the ability of its journalists to work freely. Any information about matters that could constitute grounds for censorship would be handled with kid gloves. Journalists would no longer dare to be outspoken on such subjects as religion or Pakistan's foreign policy or even those related to cyber-crime for fear of being censored. This section would lead to a grave increase in self-censorship and would have a drastic impact on the pluralism of views expressed in the Pakistani media on these subjects.

Journalists should instead be encouraged to express themselves freely and to disseminate the most diverse range of views on all subjects, especially those that, under this law, would constitute grounds for censorship.

Section 43 on prevention of electronic crimes

Section 43 would give the government the power to "issue guidelines to be followed by (...) service providers in the interest of preventing an offence under this Act." In the absence of any precision, safeguards or restrictions, this provision seems to give the authorities a

blank cheque to issue additional rules that would just compound the many problems that this law that already poses for human rights and freedom of expression.

- **Other worrisome developments**

Although there was much to be criticized in previous versions of this bill, they did at least contain many procedural guarantees. The disappearance of almost all of these safeguards in the latest draft – especially the removal of the safeguards against self-incrimination and the disappearance of any reference to the defendant's right to know the charges brought against him – is disturbing.

- **Positive aspects compared with previous drafts**

Some aspects of the bill are positive compared with previous versions released in 2014 and 2015.

- Instead of criminalizing "reckless" acts, the bill only criminalizes "intentional" acts. This is a positive development compared with previous versions of the bill, which criminalized unintentional or reckless acts. It is important that the bill makes acts an offence only if they are committed with the intent to cause harm or obtain an illegitimate advantage. It is a fundamental principle of the law that intent, especially malicious intent, needs to be established for conviction.

- In the previous version of the bill, article 48 on the powers of the security agencies legitimized all surveillance measures they might take and gave them absolute immunity from any prosecution. It has been deleted from the latest draft. This article would have had a serious chilling effect on freedom of expression and the work of journalists, could have lead to abuses by the intelligence agencies, and would have gravely undermined all the procedural safeguards provided for in the bill. The deletion of this article is a very positive step.

Authors and Credits :

Paul Coppin, coordinator of RSF Legal Committee, justice@rsf.org
Muhammad Aftab Alam, media laws expert at Freedom Network