HAUT-COMMISSARIAT AUX DROITS DE L'HOMME • OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS
PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND

Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

REFERENCE: OL
PAK 13/2015:

14 December 2015

Excellency,

I have the honour to address you in my capacity as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression pursuant to Human Rights Council resolution 25/2.

In this connection, I would like to bring to the attention of your Excellency's Government information I have received **concerning the draft "Prevention of Electronic Crimes Act" (hereinafter the "draft Cyber-crime Bill"), which allegedly contains a number of provisions that unduly restrict the right to freedom of expression and opinion in Pakistan.**

According to the information received:

In January 2015, the Pakistani Ministry of Informational Technology submitted a draft of the "Prevention of Electronic Crimes Act" (hereinafter the "draft Cyber-crime Bill") to the National Assembly for approval.

Opposition members, local NGOs and industry representatives reportedly expressed their concerns that the draft Cyber-crime Bill contained problematic provisions, including placing restrictions on human rights, conferring broad powers upon law enforcement agencies and potentially affecting businesses. The Bill was subsequently referred to the National Assembly Standing Committee on Information Technology (hereinafter "the Standing Committee") for further consideration which, on 16 April 2015, approved the legislation.

Subsequently, the Standing Committee reconsidered its decision of 16 April 2015, following complaints from human rights activists and experts as well as from members of the National Assembly, claiming their opinions and reservations regarding the Bill were ignored. However, on 17 September 2015, after making

minor changes to clauses that allegedly restricted free speech, the Standing Committee finally approved the draft Cyber-crime Bill for a second time.

The approval of the draft legislation has been severely criticized by many members of National Assembly, and the last draft of the Bill was reportedly not circulated amongst Standing Committee Members. The public, experts from NGOs, media, internet service providers, and other stakeholders who were asked to give input were allegedly never heard, and many complained that their recommendations were not considered by the Standing Committee.

Sections 3 and 4 on authorized access to information systems and on copying and transmitting data

Sections 3 and 4 of the Bill criminalize the unauthorized intentional access to "any information system or data", and the unauthorized intentional copying and transmission of "any data." Section 2(e) of the Bill defines "authorization" as including "authorization by law or the person empowered to make such authorization under the law." As such, any person accessing or visiting a website in a way that is not expressly "authorized" may be committing a crime under sections 3 and 4 and could be imprisoned for a term between 3 to 6 months, or fined between 50,000 and 100,000 rupees or both.

Section 9 on glorifying an offence and hate speech

Section 9 of the Bill criminalizes anyone who "prepares or disseminates" any type of information, including those who threaten to do so, that would "glorify an offence or the person accused or convicted of a crime" and "support terrorism or the activities of proscribed organizations, which is authorized". It also criminalizes the preparation or dissemination of information "through any information system or device" that would "advance religious, ethnic or sectarian hatred."

Section 10 on "cyber-terrorism"

Section 10 defines "cyber-terrorism" as committing or threatening to commit any of the offences listed under sections 6, 7, 8 and 9 of the Bill, which includes "unauthorized access to critical infrastructure information system or data", "unauthorized copying or transmission of critical infrastructure data", or "interference with critical system or data", when there is intent to "create a sense of fear, panic or insecurity in the Government or the public" or to "advance religious ethnic or sectarian discord." The penalty, for a person found guilty of this offence, carries a prison term of up to 14 years and/or a fine of up to 50 million rupees.

Section 2 (j)(ii) of the Bill defines "critical infrastructure" as including "any other private or Government infrastructure so designated by the Government" for the

purposes of this Act. As such, the authorities could reportedly deem any infrastructure as "critical", so that anyone who transmits any such information or data could be prosecuted as a terrorist if she or he had not been authorized to access it.

Section 18 relating to offences against a person's dignity

Under section 18 of the draft Bill, anyone who "intentionally publicly exhibits or displays or transmits any false information, which is likely to harm or intimidate the reputation or privacy of a natural person shall be punished with imprisonment for a term which may extend to three years or with a fine up to one million rupees or both."

The wording of section 18 is vague. In particular, the use of the word "likely" is problematic as it could have significant implications for individuals, including journalists, who could be prosecuted for transmitting inaccurate or partially inaccurate information that could, for example, affect the reputation of a public figure. The possibility of such a prosecution could impact investigative work and increase self-censorship, thus restricting the right to freedom of information.

Section 22 on spamming

According to section 22 of the Bill, "spamming" is defined as the transmission of "harmful, fraudulent, misleading, illegal or unsolicited information to any person without the express permission of the recipient." The specific reference to "unsolicited" makes it a crime to send an email, photo or a text message or post a photo or a comment on a social network without the recipient's prior consent. Anyone found guilty of an offence under this section can be punished with a fine up to 50,000 rupees for the first offence and up to one million rupees or a prison term of up to 3 months or both for subsequent offences.

Section 23 on spoofing

Under section 22, satire is reportedly criminalized and carries a penalty of up to three years and/or a fine up to 500,000 rupees or both.

Section 29 on retention of traffic data

According to the latest draft, a service provider should "retain its traffic data for a minimum period of one year or such period as the Authority [Pakistan Telecommunication Authority] may notify from time to time and provide that data to the investigation agency or the authorized officer whenever so required."

In relation, section 28 of the Bill allegedly permits the "authorized officer" to require any person "to provide that data" or to ensure that the integrity of the requested data be preserved for a maximum of 90 days. Moreover, section 32 of

the Bill bestows a number of wide-ranging powers on this "authorized officer", which includes the ability to "have access to and inspect the operation of any specified information system" (para. a). It also allows the officer to "have access to or demand any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such information system into readable and comprehensible format or plain version" (para. d) in addition to requiring any person "who is in possession of decryption information of an information system, device or data under investigation to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence" (para. g).

Furthermore, sections 30 and 31 of the Bill refer to warrants which are needed for search and seizure and disclosure of data if the Court is satisfied that there are reasonable grounds to believe that such material "may be reasonably required for the purpose of a criminal investigation or criminal proceedings". However, it seems from the draft legislation that a warrant is not needed to obtain access to an information system or a decryption key.

Under section 32, the powers of authorized persons are reportedly excessive and intrusive and constitute a significant threat to the privacy of citizens in Pakistan. They also constitute a threat to the work of journalists and the confidentiality of their sources.

Section 34 on the power to manage on-line information

Section 34 of the Bill empowers the Pakistan Telecommunication Authority to order service providers to "remove any information or block access to such information 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" (para. 1).

This provision is overly broad and fails to include adequate safeguards for the protection of the rights to privacy and freedom of expression. It bestows power on a statutory body or its authorized officer to block or remove any information from any website that is deemed inappropriate, without any oversight by a Court. In addition, it is unclear what is meant by the phrase "in the interest of the glory of Islam", or what constitutes "decency and morality" or how these are to be evaluated.

While I do not wish to prejudge the accuracy of these allegations, I express serious concern that the draft Cyber-crime Bill, in its current form, uses overly broad terms that lack sufficiently clear definitions, permits authorities to criminalize online expression and to gain access to Internet data without any judicial control. This could lead to the institutionalization of violations of basic rights, such as the fundamental rights to privacy and freedom of expression for Pakistani citizens, as well as to the work

and safety of media workers, including journalists in Pakistan. If adopted in its current form, the draft legislation could result in significant censorship of and self-censorship by the media, especially those critical of the Government.

Although it is legitimate to protect information systems from unauthorized access, the wording of sections 3, 4 and 10 of the Bill, in particular, is very broad, and it effectively criminalizes the accessing, copying and transmitting of any information system or data. In their current form, sections 3, 4 and 10 of the bill could have a strong chilling effect on media activities in Pakistan, pose a serious threat to the ability of journalists to work freely, especially investigative journalists, whose work precisely consists of accessing information they are not authorized to access. These provisions could also seriously deter whistleblowers who, by definition, reveal information of general interest by transmitting data they are not authorized to access, copy or transmit.

I would like to emphasize that, with regards to disclosure of sensitive information, any exceptions to the right of freedom of expression should be narrowly defined and clearly provided by law and be necessary and proportionate to achieve one or more of the legitimate objectives of protecting the rights or reputations of others, national security, public order, or public health and morals.

I am further concerned that the multiple references to penalties under the draft legislation are incompatible with article 19 ICCPR and could create a deterrent effect which may be used against the media and restrict its freedom of expression on particularly sensitive subjects. Additionally, these penalties do not meet the proportionality requirement of article 19(3) ICCPR, as they are not proportionate to the activities they are designed to sanction.

Finally, I would like to take this opportunity to express my concerns regarding the reported exclusion of civil society and the private sector from consultations and a genuine public scrutiny of the Bill prior to the vote on its adoption in the National Assembly. A lack of open and comprehensive consultation risks undermining the democratic process in Pakistan.

In view of all of the aforementioned comments, I would like to call on your Excellency's Government to take all steps necessary to conduct a comprehensive review of the "Prevent of Electronic Crimes Act (2015) ensuring its compliance with international human rights standards.

It is also my responsibility, under the mandates provided to us by the Human Rights Council, to seek to clarify all cases brought to my attention. Therefore, I would be grateful for any additional information and any comment you may have on the above mentioned allegations. I also welcome any clarifications on measures taken to ensure the compliance of the Prevention of the Electronic Crimes Act with Bangladesh's obligations under international human rights law and standards, particularly with regard to the right to freedom of opinion and expression.

Finally, in connection with the above alleged facts and concerns, please refer to the **Reference to international law Annex** attached to this letter which cites international human rights instruments and standards relevant to these allegations.

Your Excellency's Government's response will be made available in a report to be presented to the Human Rights Council for its consideration.

Please accept, Excellency, the assurances of my highest consideration.

David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Annex
Reference to international human rights law

In connection with the above alleged facts and concerns, I would like to refer your Excellency's Government to the right to freedom of opinion and expression as set forth in article 19 of the International Covenant on Civil and Political Rights (ICCPR), ratified by Pakistan on 23 June 2010, which guarantees the right to freedom of expression. Any restrictions on expression, including restrictions that strongly implicate expression, must be consistent with article 19(3) ICCPR, i.e. be provided by law, serve a legitimate government interest, and be necessary in a democratic society.

Article 17 ICCPR also provides for the rights of individuals to be protected, inter alia, against arbitrary or unlawful interference with their privacy and correspondence and provides that "everyone has the right to the protection of the law against such interference or attacks."

In paragraph 30 of its General Comment No. 34 on the right to freedom of opinion and expression, the Committee has stated that "extreme care must be taken by States parties to ensure that treason laws and similar provisions relating to national security, whether described as official secrets or … otherwise are … applied in a manner that conforms to the strict requirements of paragraph 3 [of article 19 ICCPR]." Such laws should not be used to "suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists … or others, for having disseminated such information" (CCPR/C/GC/34).

Similarly, in paragraph 38 of the same General Comment, the Committee has stated that, in circumstances of public debate concerning public institutions, the value placed by the Covenant upon uninhibited expression is particularly high. Thus, the mere fact that forms of expression are considered to be offending is not sufficient to justify the imposition of penalties. The General Comment has established that "the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty."

I would also like to take this opportunity to refer your Excellency's Government to paragraph 79 (f) of the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to the Human Rights Council (A/HRC/14/23), where he emphasizes that "Laws imposing restrictions or limitations must not be arbitrary or unreasonable and must not be used as a means of political censorship or of silencing criticism of public officials or public policies."

In paragraph 60 of the report analyzing the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression (A/HRC/23/40), the previous Special Rapporteur has noted that "the use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern." He has stated that "the concept is

broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability."

Allowing authorities to have broad discretion to shut down internet communication in response to threats is incompatible with article 19 (3) ICCPR. As I have noted in paragraph 32 of my report (A/HRC/29/32), any proposals to impose restrictions on encryption or anonymity "should be subject to public comment and only be adopted, if at all, according to regular legislative process. Strong procedural and judicial safeguards should also be applied to guarantee the due process rights of any individual whose use of encryption or anonymity is subject to restriction. In particular, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction."

In paragraph 60 of my 2015 report (A/HRC/29/32), I have recommended that "States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows. Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals."