United Nations A/HRC/36/NGO/88

General Assembly

Distr.: General
31 August 2017

English only

Human Rights Council
Thirty-sixth session
11-29 September 2017
Agenda item 4
Human rights situations that require the Council's attention

Written statement* submitted by the Association for Progressive Communications (APC), a non-governmental organization in general consultative status

The Secretary-General has received the following written statement which is circulated in accordance with Economic and Social Council resolution 1996/31.

[18 August 2017]

* This written statement is issued, unedited, in the language(s) received from the submitting non-governmental organization(s).

GE.17-15191(E)
1715191

Turkey: Secure digital communications are essential for human rights

The Association for Progressive Communications (APC) and IFEX are international networks of organisations working to support and promote human rights and freedom of expression. We submit this written statement ahead of the Human Rights Council's 36th session to express our grave concern about the growing crackdown on the use of secure digital communications, and in particular the arrest and pre-trial detention of IT consultant Ali Gharavi and non-violence and well-being trainer Peter Steudtner, together with eight Turkish human rights defenders.1 States have the obligation to facilitate the use of secure digital communications, and should not be criminalising it.

I. Importance of secure digital communications

Secure digital communications, including the use of encryption and anonymity tools, are critical to the functioning of the modern world. Guaranteed end-to-end security is necessary to the functioning of the global economy, voting systems, and a wide range of functions carried out by governments and the private sector. These tools are also essential for the exercise of human rights in the digital age. They provide individuals with means to protect their privacy, and to develop and share opinions and information without interference. They enable civil society, journalists and human rights defenders (HRDs) to carry out their work freely and securely. For members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists, survivors of gender-based violence and others to exercise the rights to freedom of opinion and expression, these tools are especially important.

In environments where discriminatory restrictions are in place that criminalise expression, and where political opposition, dissenters and HRDs are subject to surveillance and intimidation, secure communications – whether through the use of encryption, anonymisation tools like Tor, virtual personal networks or proxy servers – may be the only way in which an individual is able to safely and securely engage in HRD work.2 Beyond freedom of expression, secure digital communications are necessary in order to exercise the rights to freedom of peaceful assembly and association, to health, to security, to be free from gender-based violence, and a wide range of human rights.

II. States have the obligation to facilitate use of secure digital communications

As the UN Special Rapporteur on freedom of opinion and expression David Kaye has recommended with his 2015 report:

> With respect to encryption and anonymity, States should adopt policies of non-restriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective, require court orders for any specific limitation, and promote security and privacy online through public education. […] States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications.3

In addition, the Special Rapporteur on the right to privacy, Joe Cannataci, has encouraged governments to take a position against back doors to encryption4 and supports working with the technical community to advance "the

1IFEX. (2017, 18 July). IFEX strongly condemns charges against 10 HRDs. https://www.ifex.org/turkey/2017/07/18/turkey_july_hrd_statement

2Kaye, D. (2015). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (A/HRC/29/32), paragraph 23. www.un.org/ga/search/view_doc.asp?symbol=A/HRC/29/32

3Kaye, D. (2015). Op. cit., paragraphs 57 and 59.

4Cannataci, J. (2016). Report of the Special Rapporteur on the right to privacy (A/HRC/31/64), paragraph 60. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/262/26/PDF/G1626226.pdf?OpenElement

development of effective technical safeguards, including encryption, overlay software and various other technical solutions where privacy by design is genuinely put into practice."5 Multiple HRC resolutions have called on states to not interfere with the use of encryption and anonymity tools as part of their human rights obligations.6

III. The use of secure digital communications is under attack throughout the world

APC and IFEX are gravely concerned about and condemn the crackdown on the use of secure digital communications that we are seeing in many parts of the world. Many governments, including those of Australia and the United Kingdom, are threatening to legislate backdoors for law enforcement in encryption standards, which would substantially weaken security for everyone while increasing the likelihood of damaging attacks from bad actors.7 Other governments, such as those of Ethiopia and Turkey, are now characterising the use of encryption technologies as itself somehow proof of violent or "terrorist" activity.8

We would like to draw the Council's attention to Turkey's recent arrest and pre-trial detention of IT consultant Ali Gharavi and non-violence and well-being trainer Peter Steudtner. The arrests took place on 8 July 2017 while Gharavi, Steudtner and eight Turkish human rights defenders were gathered for a digital security and information management workshop on one of Istanbul's islands, Buyukada. Police raided the workshop, detained the participants, and confiscated electronic equipment including computers and mobile phones. Eight of the 10 individuals – Gharavi, Steudtner, İdil Eser (Amnesty International), Günal Kurşun and Veli Acu (Human Rights Agenda Association), Nalan Erkem and Özlem Dalkıran (Citizens' Assembly), and İlknur Üstün (Women's Coalition) are currently being held in pre-trial detention over accusations that they aided an armed terror group.9

Gharavi and Steudtner were arrested for simply doing their jobs – professionally imparting their skills and knowledge around technical matters – as they have done for many years with civil society groups around the world. Technical expertise should not be criminalised. Their arrests set a dangerous precedent, and are part of a broader crackdown on lawful activity in Turkey that should be part of any healthy democracy: the normal activity of an active civil society and press.

As previous HRC resolutions have emphasised, the use of secure digital communications should be available to all people, including civil society in Turkey. Instead, the Turkish government is criminalising these tools, and intentionally conflating what are standard good security practices with terrorist activity.

Ultimately, this is a failing strategy. It fails to comply with Turkey's human rights obligations by criminalising tools that are necessary for the exercise of human rights in the digital age; and it fails from a security perspective, because in the contemporary technological environment, intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online.10

5Cannataci, J. (2016). Op. cit., paragraph 50.

6See HRC/RES/34/7, paragraph 9: "Encourages business enterprises to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity, and calls upon States not to interfere with the use of such technical solutions, with any restrictions thereon complying with States' obligations under international human rights law," and HRC/RES/32/2, paragraph 13: "Emphasizes that, in the digital age, encryption and anonymity tools have become vital for many journalists to exercise freely their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use of such technologies, with any restrictions thereon complying with States' obligations under international human rights law."

7Abelson, H., et al. (2015). Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. MIT Computer Science and Artificial Intelligence Laboratory Technical Report. dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8

8See the case of the Zone 9 bloggers in Ethiopia: IFEX. (2015, 16 October). Zone 9 bloggers: Out of jail, but not free. https://www.ifex.org/ethiopia/2015/12/17/zone_nine_bloggers_profile

9Electronic Frontier Foundation (2017, 24 July). Global condemnation for Turkey's detention of innocent digital security trainers. *IFEX*. https://www.ifex.org/turkey/2017/07/28/detention-security-trainers

10See Kaye, D. (2015). Op. cit., paragraph 8, and Abelson, H., et al. (2015). Op. cit.

IV. Recommendations

To the Human Rights Council:

- **Work with states to ensure that the internet is a tool for fostering citizen and civil society participation, for the realisation of development in every community, and for exercising human rights, as per 2016 HRC resolution 32/13.**
- **In the spirit of this resolution, monitor efforts by member states to restrict the use of secure digital communications that violate their obligations under international human rights law.**
- **To the Government of Turkey:**
- **Drop the charges against Gharavi, Steudtner and the eight Turkish human rights defenders.**
- **Respect human rights online, in particular by not criminalising the use of secure digital communications and not conducting network shutdowns, censorship of online content, and surveillance of internet users.**

APC is a global organisation and network of members that work to empower and support organisations, social movements and individuals in and through the use of information and communication technologies (ICTs) to advance human rights, social justice, gender equality and sustainable development. APC has 55 organisational members and 30 individual members active in 75 countries, mostly in the global South.

IFEX is a global network of over 115 civil society groups in more than 70 countries that defends and promotes freedom of expression as a fundamental human right. IFEX exposes threats to free expression online and off, focuses on bringing to justice those who violate these rights, and advocates for the rights of women, media workers, LGBT people, artists, academics, citizen journalists, and activists.