United Nations A/HRC/27/NGO/X

General Assembly

Distr.: General
XX August 2014

English only

Human Rights Council
Twenty-seventh session
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Joint written statement* submitted by the Korea Center for United Nations Human Rights Policy, non-governmental organization in special consultative status

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

[24 August 2014]

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

Cases of the Republic of Korea on the Right to Privacy in the Digital Age[1]

1. In the Republic of Korea, there has been great controversy caused by intelligence agencies illegally wiretapping the communications of citizens[2]. The National Intelligence Service (NIS) announced that they had discontinued wiretapping of mobile communications since 2005, when the illegal wiretapping of mobile telecommunication by the NIS and its predecessor (Agency for National Security Planning) became an issue. Yet, according to the official statistics on wiretapping published by the government, wiretapping by the NIS has consistently accounted for around 97% of all wiretapping cases each year[3]. At the same time, the NIS has been trying to push ahead with revisions to the Protection of Communications Secrets Act to oblige mobile communications companies as well as other telecommunications companies designated by the government to make their networks 'wiretap-ready'. Moreover, in 2009, it was found that the NIS utilized the supply of internet along with DPI (Deep Packet Inspection) technology to wiretap all communications by targeted persons via internet connections at home and the office. A related case is currently under consideration by the Constitutional Court of Korea[4].

2. In addition to the interference of communications, freedom of anonymous expression on the internet and mobile platforms is extremely limited in Korea. The internet real-name verification system[5], which was pointed out as an issue by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, was ruled as unconstitutional by the Constitutional Court in 2012 and ceased to take effect. However, Korean citizens are still required to undergo real-name verification in their everyday lives, such as when using internet bulletin boards and video game services, or when subscribing to mobile phone plans[6]. This shows that the Korean government has not implemented the recommendations of the Special Rapporteur to ensure that individuals can express themselves anonymously. It is worth noting that cases of personal data leakage increase as more government agencies and private institutions collect personal data for real-name verification[7]. Personal data leakage usually involves the leaking of resident registration numbers, which are issued to Korean citizens upon birth and remain identical for the rest of their lives; this means, using these numbers, it is possible to steal the identity of individuals or track their internet activities.

---

[1] Korean Progressive Network 'Jinbonet' NGO(s) without consultative status, also share the views expressed in this statement.

[2] http://act.jinbo.net/drupal/sites/default/files/ONI_report_Korea_090220_A4_english.pdf

[3] Relevant ministries such as the Ministry of Science, ICT and Future Planning have been semiannually publishing wiretapping statistics by institution.

[4] http://english.hani.co.kr/arti/english_edition/e_national/496473.html

[5] A/HRC/17/27/Add.2. Mission to the Republic of Korea

[6] Real-name verification is a system where an individual verifies identity by submitting his or her name and resident registration number. Real-name verification can be done through public services such as community service centers or private commercial services such as mobile phones, credit cards, public authentication certificates (electronic certificate), etc. These institutions are designated by the government.

[7] In 2013, the population of Korea was 50 million and the economically active population was 25 million. There continues to be large scale personal dataleakages. There were 18 million cases from the website Auction in 2008, 35 million cases from SNS and messenger services provided by the portal site Nate in 2011, 13 million cases f rom the internet gaming company Nexon in 2011, and 104 million cases from 3 credit card companies in 2014. These services have collected and retained resident registration numbers of Korean citizens according to relevant laws.

Such personal data collected by websites or telecommunications companies are being provided to intelligence and investigative agencies without court examination[8].

3. The system of data retention of communication metadata[9], which was found unconstitutional by the Court of Justice of the European Union, is still in effect in Korea[10]. In addition, investigative agencies do not undergo strict court examination when collecting location data from mobile phones or the internet, a problem which has led to the abuse of this system by investigative agencies. In 2012, the prosecution and police tracked in real-time for months the location data from mobile phones of activists who organized the nationwide Hope Bus march to show support for a female worker who had been in aerial protest for 150 days. Also, in 2013, the police attempted to arrest the leaders of the Korean Railway Workers' Union on strike by tracking in real-time the mobile phone locations and internet IP addresses of the workers and their spouses, parents, and children. Appeals have been filed to the Constitutional Court in regards to these cases and are currently under consideration. In addition, constitutional appeals have been filed against 'mobile base station investigations'[11] that involve collecting all mobile phone numbers whose signals were detected by mobile base stations near assembly areas, for the purpose of indentifying assembly participants.

4. The current digital environment is restricting the freedom of Korean citizens to communicate using forms of electronic communication without fear of invasion of privacy. In order to effectively protect citizens' right to privacy from state surveillance in the digital age, it is necessary to establish an independent oversight body. Still, the two main institutions hat are expected to perform that role, the National Human Rights Institution and Personal Information Protection Commission, are vulnerable to political pressure[12].

5.The Republic of Korea has achieved great technological progress, especially in the field of Information Technology (IT), along with its rapid economic growth. However, there are some areas of concern from a democratic and human rights perspective, also illustrated by the case in which an intelligence agency intervened in domestic politics, namely the past presidential elections[13]. We are concerned that, in the socio-political context, there is a high possibility for IT to be misused to carry out state surveillance and commit violations of the right to privacy. We welcome the UN General Assembly resolution[14] and the report of the Office of the High Commissioner for Human Rights[15] on the right to privacy in the digital age, and we emphasize the urgent need for these recommendations to be implemented by the RoK.

---

[8] According to the statistics published by the Ministry of Science, ICT and Future Planning, in 2013, there were 9,574,659 official cases in which personal datawas provided to intelligence and investigative agencies without warrants.

[9] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

[10] According to the Enforcement Decree of the Protection of Communications Secrets Act, data from internet services,
landline phone calls, and mobile communication services are required to be retained for 3, 6, and 12 months respectively.

[11] Mobile base stations in densely populated areas provide more than 10,000 mobile phone numbers per request by investigative agencies.

[12] See "Human rights commission to face ICC demotion", http://www.koreatimes.co.kr/www/news/nation/2014/04/113_154823.html ; The Personal Information Protection Commission only has the right to examine, while the government possesses authority over budgeting and human resources and the Ministry of Security and Public Administration is responsible for functions such as investigation, corrections orders, etc.

[13] A/HRC/25/NGO/86. Joint written statement submitted by the People's Solidarity for Participatory Democracy and MINBYUN-Lawyers for a Democratic Society, non-governmental organizations in special consultative status

[14] A/RES/68/167. http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1

[15] A/HRC/27/37.
http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

Korean Progressive Network ‘Jinbonet’ NGO(s) without consultative status, also share the views expressed in this statement.