

WHAT ARE HUMAN RIGHTS?

DONATE

**HOME** 

ABOUT US

ISSUES

HUMAN RIGHTS BY COUNTRY WHERE WE WORK

HUMAN RIGHTS BODIES NEWS AND EVENTS

PUBLICATIONS AND RESOURCES

English > News and Events > DisplayNews

# Statement to the media by the United Nations Special Rapporteur on the right to privacy, on the conclusion of his official visit to the Republic of Korea, 15-26 July 2019

Korean Version (Word Format)

Seoul, 26 July 2019

- 1) I would like to thank the Government of the Republic of Korea for its invitation to visit the country from 15 to 26 July 2019, and for its generous cooperation. I would especially like to thank the Human Rights and Social Affairs Division of the Ministry of Foreign Affairs for its efforts supporting my visit.
- 2) The views expressed in this statement are of a preliminary nature. My final findings and recommendations will be presented in my report to the United Nations Human Rights Council in March 2020.
- 3) During my visit, I assessed the situation of the right to privacy in the Republic of Korea. I studied ongoing reforms, existing mechanisms to prevent violations of the right to privacy and heard concerns expressed by civil society organizations, experts and other actors. I also received useful information on best practices being carried out in the Republic of Korea.
- As part of my fact-finding mission, I visited Seoul, Jeju Province, Daegu and Miryang. I met with senior officials of the Government at the national and provincial levels, the legislature, the judiciary, law enforcement, intelligence, the national data protection authority, human rights institutions, academia and non-governmental organizations. I would like to thank all of them for their time and their valuable inputs received both before and during the visit, and look forward to a fruitful cooperation.

## Surveillance

- 5) In my work, I examine the activities of police agencies and intelligence services in order to determine whether any privacy-intrusive actions, and especially surveillance measures, are provided for by law and are necessary and proportionate in a democratic society. There is copious evidence, either received from civil society in the country, or available in the public domain or otherwise procured independently, of abusive behaviour by both the Police and the National Intelligence Service.
- 6) The senior officials of the National Police Agency whom I met did not comment on specific cases which are currently sub judice but neither did they deny past abuses. Moreover, they undertook to make all efforts to make up for and prevent any past mistakes from being committed again in future. Efforts include new regulations to prohibit police surveillance against civil organizations and

setting up a new compliance team which monitors the legitimacy of activities of intelligence officers.

- 7) The National Intelligence Service also accepted to meet me and I was pleased to carry out very open and frank discussions with senior officials. My mandate was therefore able to give the NIS the opportunity to hear their side of the story and to listen to how it proposes to prevent past mistakes from being committed in future. I can, therefore, conclude that media reports about significant recent internal reforms by incoming Director Dr. Suh Hoon are correct and that significant progress has been achieved with regard to human rights protection since he took over. The NIS "humbly accepted" the evidence, which proves the multiple allegations brought against it for the period up to 2016 and was very open to discuss options which would help ensure that no similar infringements of privacy would occur in future.
- 8) I have taken note of the very detailed evidence presented by civil society as well as the published results of the findings, decisions and recommendations of the Constitutional Court, the Supreme Court, the National Human Rights Commission and various official inquiries undertaken by the Government or on its behalf over the past two decades. When taken together with the evidence collected in person during this visit, these elements point to systemic and multiple serious infringements of the right to privacy by both the National Police Agency and the National Intelligence Service up to the period of late 2016 and possibly the first half of 2017.
- 9) The National Intelligence Service has commenced its reform in a significant manner since June 2017 with a number of measures initiated by its new Director:
- a) the abolition of its domestic intelligence collection function
- b) the removal of intelligence officers embedded in various areas of government.
- c) the reinforcement of its legal unit by recruiting new staff in considerable numbers
- d) appointing legal compliance officers in each division;
- e) creating a Reform Committee with participation from outside the service including leading lawyers, academics and members of civil society;
- f) Creating internal inquiries about past misdeeds;
- g) Suspending use of a number of privacy-intrusive technologies including RCS;
- h) Reinforced human rights and legal compliance training in both induction and regular in-service courses;
- 10) It is also clear that the National Assembly of Korea is well aware of the problems of abuse and accountability, especially in the National Intelligence Service and has reported the existence of up to sixteen (16) pieces of draft legislation intended to thoroughly reform the NIS.
- I cannot but echo many of the requests for reform made by many members of the National Assembly as well as those of Korean civil society. I am seriously concerned, in particular, about the lack of effective independent oversight of surveillance and investigatory powers that apparently exists in the country.
- An essential element of oversight already exists in the important work carried out by the Intelligence Committee of the National Assembly of Korea. That however is insufficient insofar that the Committee does not possess either the legal authority or the resources to fully audit, in-depth the conduct of a specific case, and does not have full unfettered access to the contents of a case file.
- 13) In the light of the above, I therefore draw the attention of both the Government and the National Assembly to the following issues and invite them to take urgent action and maximise the opportunity afforded by upcoming debates in the National Assembly about legislation currently in draft form.
- 14) The legal basis and the regulatory framework for surveillance by both the National Police Agency and the National Intelligence Service is inadequate and is in need of urgent and

comprehensive reform;

- The internal audit functions of both the National Police Agency and the National Intelligence Service of the Republic of Korea should be significantly reinforced by the creation of standing teams including representation of the Director of Human Rights Protection of the respective agencies, which would be empowered and tasked with the end-to-end audit of specific cases, selected both on an "own initiative basis" and a "random sampling" basis, in addition to investigation of complaints brought against individuals or units.
- The current powers granted by law to the Intelligence Committee of the National Assembly are too limited and, in practice, prevent it from carrying out effective oversight of the National Intelligence Service. They should be widened considerably;
- The National Intelligence Service should conduct an in-depth revision of its culture and practices of opacity, whether self-developed or imposed by law. Making sure that only information that needs to be kept secret is in fact secret, would allow Korean society to better understand the role and working methods of the National Intelligence Service. Ultimately, and together with strict oversight and adherence to the law, it would help the National Intelligence Service to gain trust from Korean citizens.
- 18) There should be created a new independent full-time body which could be called the Surveillance and Investigatory Powers Commission (SIPC) whose work should complement that of the Intelligence Committee of the National Assembly of Korea.
- 19) This new independent entity (SIPC) should:
- a) contain a blend of senior judges (serving and/or recently retired), ICT technical staff and experienced domain experts with a successful track record of working in the police and/or the intelligence services, (principle of multi-disciplinarity) tasked with oversight both ex ante and ex post;
- b) employ people in adequate numbers (principle of adequate resourcing)
- c) who would have full authority provided for by law (principle of full legal basis)
- d) to carry out frequent and regular (at minimum once a month) snap-checks of both intelligence agencies and police services (principle of full authority and complete unfettered access) in order to
- e) assess whether any surveillance being carried out is legal, necessary and proportionate (principles of legitimacy, necessity and proportionality).
- f) In line with emerging international best practise, this new oversight body should have full and permanent remote electronic access to all databases held by the intelligence and police forces it oversees (principle of full electronic access).
- g) report independently to the legislature and not to the executive and thus also be subject to the oversight of the Intelligence Committee of the National Assembly of Korea (principle of independence from the Executive branch of Government)
- h) be assigned an independent line budget in the annual financial estimates approved by the National Assembly such that is amply sufficient for it to carry out its duties; (principle of financial independence)
- i) be composed of a part-time Commission appointed by a combination of existing institutions and not by Government which would oversee the transparent appointment of a full-time Chief Executive for our purposes here called the Commissioner and the remainder of the staff of the new independent entity; (principle of appointment of SIPC Commissioner and staff being carried out completely independent of Government)
- j) The method of appointment of the SIPC is a subject which should also receive close attention and be subject to public consultation, given the apparent lack of trust in Government and politicians evident in Korean society. It is recommended that some of the options that would be explored would

#### include that:

- i) The SIPC would be composed of the following members:
- ii) A senior serving judge nominated by the President of the Constitutional Court, who would act as Chair of the SIPC;
- iii) A senior serving judge nominated by the Chief Justice/President of the Supreme Court in consultation with the Administrative Council of Justice/Judges or similar body which may exist in Korea;
- iv) A lawyer experienced in human rights matters nominated by the Korean Bar Association in consultation with the Council of the KBA;
- v) A retired senior police officer of unimpeachable integrity nominated by the President of Korea;
- vi) A retired senior Intelligence Office of unimpeachable integrity nominated by the leader of the Opposition of Korea (the same person as would identified by Article 127 of the Korean Constitution)
- vii) The full-time Chief Executive of the SIPC to be appointed by the SIPC members would preferably (but not necessarily) be a recently retired senior Judge of unimpeachable integrity, preferably with experience of dealing with intelligence, police and surveillance cases;
- I have noted calls by civil society to subject to judicial overview the current unfettered access of police and intelligence services to meta-data about telephone calls and other communication means. Requests for metadata that are considered sensitive do require a court warrant, and amount to around 300,000 requests per year. The figures of metadata requests considered non-sensitive and therefore not requiring a court warrant, however, are staggering, ranging from 6.4 million to 9.3 million per annum and suggest that access to such data is sometimes requested casually and most probably in many cases without being really necessary. It would prima facie appear that the number of requests for access made is possibly much higher than in most other democracies. It may be a good idea to subject these requests to judicial oversight, or very preferably the new SIPC, even if only to improve privacy protection by discouraging casual access and cutting down the sheer number of requests currently being made. If, however, the current numbers persist, it is estimated that 500-800 new judges or persons with legal training and of judicial standing with special ad hoc training on intelligence matters, would need to be recruited in order to cope with the workload (6.4 million requests) which would tend to have to be tackled on a 24/7 basis.
- I have noted with concern that, on several occasions, activists, protesters or members of social movements have been subjected to surveillance by the police that was either unnecessary and/or disproportionate. The arbitrary surveillance of activists and human rights defenders are not new: in 2013, the Special Rapporteur on the situation of human rights defenders, Margaret Sekaggya, asked the Government to conduct prompt and impartial investigations of all allegations of surveillance against human rights defenders and hold perpetrators accountable (A/HRC/25/55/Add.1).
- 22) Perhaps the most compelling case I have witnessed was that of the families of victims of the SEWOL ferry disaster on 16 April 2014, where 304 persons died and 5 went missing, most of them school children. The accident was found by the courts to be the result of negligence by authorities and the company who owned the ferry. The captain was also sentenced to 36 years in prison for gross negligence. However, when families of the victims initially organized themselves to demand an investigation and fight for compensation, the Government severely obstructed any progress and the Defense Security Commands (a body of the Korean Armed Forces) carried out surveillance on the victims' families. I positively note that, due to the excesses of the Defense Security Command in this and other cases, that branch of the Armed Forces has been subjected to deep reform, rebranded and stripped of their competencies on domestic surveillance. The evidence presented so far seems to indicate that the Defense Security Command unfoundedly labelled the families of survivors as sympathizers of the DPRK Government, and illegally collected large amounts of personal data (including online shopping information). They also followed family members and disguised themselves as victims' families in order to spy on them. I met with one of the family members and was appalled to see that the victims of the worst disasters in the country's recent history were, again, painfully

victimized through illegal surveillance and harassment by the State. Those who should have been consoled, protected and compensated by the State in such a difficult moment, were instead seen as its enemies. The responsibility of the violations inflicted on them must be fully clarified and those found responsible must be held accountable.

I also met with members of social movements in Daegu and Miryang who have opposed the construction of an anti-missile defence site and of electricity lines. Instead of engaging in dialogue and negotiation, it seems that the State and/or parastatal agencies opted for confrontation and imposition, sometimes through a disproportionate police presence and the intensive surveillance of protesters (including physical surveillance of the private domiciles of elderly protesters at night), even of those who have legitimately exercised their freedom of assembly on a peaceful manner and could hardly pose a security threat. While I can understand the strategic importance of anti-missile defense systems and vital power lines, only those protesters who break the law and pose a serious threat to security should be investigated by the police. Attempts to dissuade protesters through arbitrary surveillance and police harassment violate not only their right to privacy but also their right to freedom of expression and assembly. I welcome the efforts of the Government to investigate the case through the Truth Commission on Human Rights Violations of the National Police Agency.

# Privacy and children

- I have noted that, although it is a fading trend, some elementary school children are still encouraged to keep a personal diary for the improvement of their written expression. Some of them are forced to show it regularly to the class teacher. In this instance, I would advise that the practice of keeping a diary can be preserved as long as the children are accurately informed of the fact that the content of the diary can and will be examined by the teacher and should it contain sensitive information related, for example to child abuse, the teacher has a duty to act upon it.
- Another concern I have received testimony about was related to the mandatory installation of CCTVs in child-care centres. I assess that the current safeguards in place related to how the CCTV footage can be examined are adequate. The number of requests granted is very small. For example, in Daegu only 2 requests have been granted in 6 months for 2 educational units out of 120.
- I have also received complaints that there were cases in which the CCTV footage was leaked to the media during investigations together with the victim's name, age, address and school name. In the case of a leakage that infringes on the individual's privacy the Press Arbitration Commission using the "recommendation system" reviews the content post publication and issues a non-compulsory recommendation that is published on the homepage of the Commission. The Press Arbitration Commission has also issued a set of standards related to the disclosure of personal information in the media. In addition, the Korea Communications Standards Commission can assess possible violations by broadcasters, which can lead to binding measures by the Korea Communications Commission, such as monetary penalties and orders to remove or correct information. We shall be considering the extent to which the content of recommendations by the Press Arbitration Commission is of sufficient deterrence value. We shall also be considering the extent to which the current framework results in sanctions which are timely and whether any existing recommendations should be made compulsory. The relationship to the imposition of severe fines to media outlets will also be further assessed.
- I have assessed complaints from civil society that in a number of schools there exist guidelines, which sanction and impose punishments for dating between school students. The facts of the matter are still being verified since it would appear that some of the data on which some of the complaints relied (2009-2013) may in fact be too dated and the problem may have since been largely resolved. Since 2013 the Ministry of Education has introduced a set of official guidelines on the circumstances in which students can be disciplined and the steps which need to be taken in these cases. It has been reported to me that the procedures detailed in the manual have contributed to preventing the taking of arbitrary disciplinary measures which may have been related to the student's sexual preferences and/or dating activities.

## **CCTV** and facial recognition

28) There does not appear to be any permanent deployment of facial recognition technology and

none of the Government agencies, including the National Police Agency reported any intention to introduce such systems into public spaces in the near future.

29) I endorse the recommendations made by the Korean National Human Rights Commission to introduce legislation that would provide a proper legal basis for the creation of a national centre integrating CCTV surveillance from all over municipal CCTV systems across Korea.

#### **Data protection**

30) The law on Data Protection (PIPA) is relatively strict and follows standards which in many cases come close to those of the EU's GDPR. However, the issue of the true independence of the Personal Information Protection Commission (PIPC) has been raised as a matter of concern since it does not receive its own assured separate line budget with a statutory authority to recruit its own staff independently of the Government departments, which it is also expected to oversee. I, therefore, recommend that this anomaly be removed and that the PIPC's autonomy and independence be significantly reinforced through statutory and budgetary provisions, which would allow for completely independent recruitment and staffing. This reform would help the Republic of Korea move significantly closer to the international gold standard established in Convention 108+ in its latest version opened for signature on 10 October 2018. I strongly recommend that Korea seek accession to this international standard-setting convention, which is today embraced by more than 55 countries from around the world. Reinforcing its Data Protection Authority in the manner here recommended would also doubtless further improve Korea's chances of speedily obtaining an adequacy assessment by the European Union in relation to the GDPR. Furthermore, I also recommend that the PIPC be allowed to impose - and collect the revenue from - administrative fines, which should be set to a maximum of 4%-5% of global turnover of the organisation concerned.

## Health and social security data

- In 2010 the Ministry of Health and Welfare introduced the 'Social Security Information System' (SSIS) for the management of multiple welfare benefit schemes through one electronic system. I assess that the system includes adequate safeguards in terms of how the data is being collected from the utility companies and similar government agencies, how the risk analysis is being done and how the information is used when reaching out to potential beneficiaries of the system.
- 32) In spite of receiving requests by other countries, the Korean authorities are in agreement that medical data should, for the time being, not be considered in the scope of international and regional trade agreements. I thoroughly commend this approach, which should serve to prevent the further commodification of sensitive medical data.
- Access to medical data is given only in very limited cases and only when it leads to a strengthening of the right to health. The request for access is reviewed by the Deliberation Committee, which includes experts in privacy, human rights, life and ethics and the decision-making process is transparent. I here draw the attention of the Government of the Republic of Korea to the full version of the guidelines and recommendations on health-data produced by my mandate which should be followed when considering all uses of such sensitive personal data.

#### Right to privacy of HIV/AIDS-positive persons

I have received reports of violations of the right to privacy of persons living with HIV/AIDS (PLWHA). For example, the AIDS Law of 1987 criminalizes the non-disclosure of HIV/AIDS positive status to sexual partners, irrespective of intent or whether a contagion happens. The Special Rapporteur on the right to health has noted that the criminalization of the failure to disclose HIV/AIDS status is counterproductive from a public health perspective and can violate the right to privacy (A/HRC/14/20). PLWHAs in detention have also had their right to privacy violated when their HIV/AIDS positive status was openly disclosed as "special patients", an expression that inmates and guards knew referred to them being HIV/AIDS positive. I note positively that the Ministry of Justice has acknowledged errors in the management of PLWHAs in prison. It has stopped using the "special patients" banners and is working on raising awareness among its officials in order to improve the respect for their rights, including "a video for correctional officials and inmates to reduce prejudice and

negative awareness against HIV infection". Also, persons found to have acquired HIV/AIDS are automatically discharged from the Armed Forces, instead of being offered a position compatible with their condition. Men at the age of conscription found to be HIV/AIDS positive are also barred from serving in the Armed Forces.

### Right to privacy in the workplace

- 35) During my visit I have observed a lot of concern regarding the monitoring of workers through electronic devices such as CCTV and mobile phone applications. The use of CCTV footage for disciplinary actions against workers is raising problems in various industries.
- I have been pleased to note that PIPA already makes reference to this practice and bans the installation and operation of any visual data processing device in open places except for very specific circumstances. The National Human Rights Commission has also asked for measures to be adopted that would ban the use of CCTV for labour monitoring.
- 37) These recommendations have been taken on board by the Korean government, which has now introduced a ban on workplace harassment in accordance with the revised Labour Standards Act, which takes effect on July 16, 2019. The now amended legislation prohibits harassment at workplaces, which would also include the monitoring of workers through visual devices, and imposes obligations on employers to establish a system to prevent and respond to bullying in the workplace.

## New economic activities and Smart City in Jeju province

- 38) On my visit to Jeju Special Self-Governing Province, I met with the Provincial Government's Future Strategy Bureau. I learnt about the Government's innovative projects on drones, electric vehicles, blockchain, cryptocurrencies, etc. Some of these projects form part of the central Government's "regulatory sandbox", an initiative that allows companies for flexibility in their compliance with legislation in order to foster innovation.
- While attempts to promote innovation and stimulate Jeju's (and the Republic of Korea's) economy are commendable, I was concerned to see that none of the Government's plans include Privacy Impact Assessments (PIAs) prior to their implementation. I understand that PIAs were not carried out because, on the judgement of the Provincial Government of Jeju, the plans did not affect the data 50,000 persons, which is the threshold established by law. Considering the considerable potential impact of some of these projects on the right to privacy, it is urgent that such PIAs are conducted as soon as possible, and in any case before the projects enter an implementation phase, even if currently not mandated by law. Each PIA should ensure that the projects concerned respect and indeed embed the principles of "privacy by design" and "privacy by default".
- I would also like to point out that Korea's data protection framework cannot be seen as an obstacle to innovation and economic growth. On the contrary, the strict adherence to the existing data protection framework is essential to ensure that the country's development, especially in relation to new economic fields and activities, takes place in a context of legal certainty and in full respect of users' right to privacy. Data protection legislation is the product of decades of legislative and academic debate, of the tireless work of experts, civil society and international organizations, so I would advise against conducting experiments that may risk weakening the safeguards that have been so hard to build.
- 41) The Provincial Government is also planning a Smart City project in Jeju, as an attempt to favour business investment in the island, especially in its prominent tourism sector. I have talked about the risks of Smart Cities before: by installing smart sensors to track persons' activities in the city and aggregating the big amounts of data already being collected from them, Smart Cities could subject its inhabitants to a regime of surveillance even more intense than the one they are already undergoing. Therefore, I would recommend the Government to develop safeguards in order to prevent its Smart City project subjecting citizens to the excessive collection of their data by, first, completing a Privacy Impact Assessment. This PIA should be done in cooperation with civil society, especially local communities, and renewed each year because the Smart City is a quickly evolving concept. Other safeguards could be giving individuals the option to be less "surveillable"; developing and adopting disincentives for automated profiling; integrating Privacy by Design and Privacy by Default principles in

the project. Finally, I would like to recommend the Government to bear in mind that data produced by citizens, should primarily benefit them. The Government told me that the primary objective of the Smart City was to create an environment attractive to business investment, but that should not prevent having the citizens at the centre of its design. Therefore, the improvement and rationalization of city infrastructure and public services should also be primary objectives of data collection.

# **LGBTI** rights in the Armed Forces

- 42) I have received reports that LGBTI persons are subjected to violence, discrimination and to violations of their right to privacy in the Armed Forces of the Republic of Korea. While same-sex relations do not constitute a criminal offence in the country, article 92-6 of the Military Criminal Act, prohibits sex between men. As a result, it has been reported to me that members of the armed forces are questioned, sometimes under threats and intimidation, about their sexual orientation, sex life, and even the identity of their sex partners, which constitutes a violation of their right to privacy. The Armed Forces have also confirmed wrongly using dating apps to identify male military personnel who had had sexual intercourse with other male members of the Armed Forces during investigations in 2017 (the Ministry of National Defense has confirmed having investigated 28 individuals, a number that goes up to 50 according to civil society reports we have received), and attempted to intimidate some of them to hand over their mobile phones in order to identify their sex partners. The Ministry of National Defense stated that, following also the recommendations of the National Human Rights Commission, the investigatory procedures within the Armed Forces have been reviewed in order to make them less intrusive and less intimidating. I am concerned that LGBTI individuals cannot serve in the Armed Forces without fear of violence and harassment, and that some of their superiors may occasionally subject them to degrading questionings on their intimate life, which should be of no concern of the State. Considering the fact that the military service is compulsory for all men in the Republic of Korea, I am appalled to learn that virtually every non-heterosexual man will have to endure such a regime of fear for a minimum of 21 months of their life. If there is a need to impose restrictions in the private sphere of members of the Armed Forces in certain exceptional circumstances, those should be applied equally to heterosexual and same-sex relations, as all discrimination based on sexual orientation is contrary to the human rights obligations of the Republic of Korea.
- I am confident that the Armed Forces of the Republic of Korea will soon leave behind discriminatory practices that have no place in the 21st Century, as recommended by several United Nations bodies. Even before the Constitutional Court decides on the issue, the Government should take the initiative, not only to repeal article 92-6 of the Military Criminal Act (and immediately halting all related investigations), but also training members of the Armed Forces on sexual diversity, so that LGBTI individuals can serve without fear of violence or discrimination.

#### Gender-based cyber violence

- I commend the very positive good practices developed in Korea by both civil society and the Government in the area of on-line gender based violence. Of particular note in the civil society sphere is The Korea Cyber Sexual Violence Response Centre (KSCVR) which mainly focuses on "cyber sexual violence". Cyber Sexual violence is a form of online gender-based violence, which violates numerous rights, the right to privacy included. Women's right to privacy is adversely affected in online spaces. In the case of illicit videos circulating online, victims are forced to continuously suffer unless those videos are removed from the Internet. Therefore, deletion support is critical for the recovery of victims.
- In a move which complements the services provided by KSCVR, the Korean Government recognised that there is a limitation to what the existing counselling centres for sexual violence victims can do for digital sex crime victims, given that they suffer different problems from victims of rape and other sexual assault. Therefore, a separate state-led supportive organization was needed to provide specialized support for victims of digital sex crimes. To this end, the Korean Government opened the Digital Sex Crime Victim Support Centre on April 30, 2018, which provides comprehensive services such customized counselling, deletion and investigation support, and legal and medical assistance.
- The Korean Government formulated the Comprehensive Measures against Digital Sex Crimes

in September 2017. For the comprehensive measures, the Government and the National Assembly revised five acts so as to expand the scope of offenders, introduce stricter punishment, and lay the legal foundation for prompt deletion

Home Site Map CONTACT US

Frequently Asked Questions

© OHCHR 1996-2021

OHCHR on Social Media

**OHCHR** Memorial

Employment

Mobile App