



General Assembly

Distr.: General
17 October 2022

English only

Human Rights Council

Forty-sixth session

22 February–19 March 2021

Agenda item 3

**Promotion and protection of all human rights, civil,
political, economic, social and cultural rights,
including the right to development**

Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, on his visit to the Republic of Korea

Comments by the State*

* The present document is being issued without formal editing.



Comments by the Republic of Korea on the Report of the Special Rapporteur on the right to privacy

I. Introduction

1. The Republic of Korea (ROK) welcomes the visit of the UN Special Rapporteur (SR) on the right to privacy and is pleased to have had a constructive dialogue with the SR during his visit.
2. The Government of the ROK is grateful to the SR for his recognition of our efforts to progressively realize the right to privacy and implement relevant policies. The Government takes note of his valuable recommendations, in particular, to improve its institutional framework to protect the right to privacy.
3. The Government appreciates the opportunity to comment on the report of the SR and would like to comment as follows.

II. Surveillance

4. With regard to paragraph 9 of the report pointing out that efforts of the National Intelligence Service (NIS) to protect human rights such as the right to privacy were insufficient in the course of carrying out its duties, the NIS has commenced a number of reform measures as follows to prevent the recurrence:

- (a) The abolition of divisions tasked with internal intelligence function;
- (b) The suspension of using privacy-intrusive technologies; and
- (c) The reinforcement of its personnel's legal compliance through appointing an

officer to support legal compliance in each division and providing training courses on human rights.

5. In particular, the amended National Intelligence Service Act, effective as of January 1, 2021, incorporates the abovementioned measures with:

- (a) The exclusion of the article on internal security function and criminal investigative authority against communists (with the criminal investigative authority being abolished as of January 1, 2024) from the Act;

- (b) The prohibition of the establishment of a division that may have any possibilities for engaging in politics, in order to prevent the NIS from being involved in politics or human rights abuse;

- (c) The introduction of articles on crimes of illicit interception and location tracking; and

- (d) The creation of guidelines for intelligence activity that define principle, scope, procedure of its duties and obligation to report to the Intelligence Committee of the National Assembly.

6. Overall, the Act includes amendments to improve the NIS's performance to ensure that human rights such as privacy are rightfully protected. Also, enforcement decrees of the Act have been amended soon after.

7. With the implementation of the amended Act, the NIS will suspend any privacy-intrusive work related to domestic intelligence collection and prohibit unauthorized interception and location tracking that are not compliant with the Protection of Communications Secrets Act and the Act on the Protection, Use, etc. of Location Information. The NIS will spare no effort to not compromise the value of protecting human rights such as public privacy in the process of performing its duties.

8. Besides the amendment of the National Intelligence Service Act, the Government will continue its endeavors to strengthen the legal basis for protecting the right to privacy and other human rights, in relation to paragraph 54.
9. The NIS's intelligence collection is based on laws including not only the National Intelligence Service Act but Act on Counter-terrorism for the Protection of Citizens and Public Security, Protection of Communications Secrets Act, Telecommunications Business Act and Personal Information Protection Act. Its performance is also in accordance with the executive orders of each sector including security, counterintelligence, cyber-security, and space intelligence security.
10. The above-said laws and regulations have been constantly reviewed and amended to encompass the content aiming to strengthen the protection of privacy and human rights of the public.
11. Complying with the limits set in the aforementioned laws, the NIS has been and will continue strengthening internal inspection to make sure that no activities are conducted above and beyond the call of duty.
12. In addition to the abovementioned efforts of the NIS, there has been legislation on prohibiting the police from collecting intelligence on political and private sectors that are unrelated to public safety or risk prevention.
13. With a bill on the amendment of the Police Act passed by the National Assembly on December 9, 2020, the police have been reformed with a more clarified scope of intelligence activities as well as punishment regulations for political involvement established.

III. Oversight of agencies carrying out surveillance

14. Paragraph 20 pointed out the lack of effective independent oversight of surveillance and investigatory powers. The Intelligence Committee of the National Assembly monitoring the NIS's intelligence collection is one of the standing committees of the Korean National Assembly which reviews the enactment and amendment of laws that serve as the fundamental basis of the NIS's duties and budget and settlement.
15. According to the National Assembly Act and the Act on Testimony, Appraisal, etc. before the National Assembly, the Committee may request the NIS to submit related data and information in case of reviewing, auditing, and inspecting laws regarding the NIS's organization and duties as well as its budget and settlement. The National Intelligence Service Act stipulates that it must provide its full cooperation with the review and submission of related materials and responses.
16. According to the amended National Intelligence Service Act, effective as of January 1, 2021, which strengthened the Committee's authority to control the Service, the NIS shall report to the Committee when a major national security issue arises, or when more than two-thirds of the members of the Committee request a report on a specific issue; and the NIS shall report the budget execution to the Committee on a quarterly basis. Overall, with the amendment of the Act, the Committee's authority to control the NIS has been strengthened.
17. The Committee has been stepping up its oversight of the NIS to protect human rights including the public's privacy. In this regard, the NIS will continue providing the Committee with requested materials to the maximum extent possible and complying with the laws and requirements regarding the supervision of the Committee to ensure that the human rights of the citizens are not infringed.
18. In the case of the police, the National Police Agency (NPA) has designated a Director of Human Rights Protection within the agency to be in charge of protecting and investigating human rights conditions when conducting police activities.
19. The NPA will strengthen its internal management by increasing the number of human rights investigators within the year of 2021 and is planning to designate a Director General of Human Rights Policy as the overseeing body of human rights policy in the police, who will be hired among outside experts.

IV. COVID-19 and Personal Data Collection

20. In relation to paragraphs 41 through 53 on the measures taken by the Government as its responses to the spread of COVID-19, the Government would like to make it clear that all disclosure of information related to confirmed cases is made on the basis of the Infectious Disease Control and Prevention Act which stipulates that the public has the right to know the information about situations on ongoing infectious disease outbreaks, the prevention and control measures being taken, how to protect oneself in such situations, and that the state and local governments must promptly disclose relevant information to the public.

21. The Infectious Disease Control and Prevention Act requires that, when a crisis alert of Level 2 (Yellow or Caution) or higher is issued in accordance with the Framework Act on the Management of Disasters and Safety due to an infectious disease outbreak, the governments must ensure that the information related to disease control such as the locations traced, means of transportation used, healthcare facilities visited, and contact tracing progress updates are made promptly available to the public. In general, such information had been posted online by the Minister of Health and Welfare.

22. The Government recognized the importance of privacy protection and provided guidance to all local governments several times to prevent the unnecessary disclosure of personal information. To this end, the Government executed and distributed several official documents during the first half of 2020 pertaining to the following:

(a) Request to practice thorough security precautions in handling personal information and to ensure that the collected information is used only for the purpose for which the collection was made (February 23, 2020);

(b) Guidance to not disclose personally identifiable information, detailed residence addresses, and names of workplaces when disclosing the locations of confirmed cases and providing guidance on the scope of information disclosure (March 14, 2020);

(c) Provision of guidance on how long the disclosure should be made available, specifying that the information must be deleted or redacted from public spaces after 14 days from the last contact of the confirmed individual (April 12, 2020);

(d) Instruction to exclude personally identifiable information in public disclosure (May 20, 2020); and

(e) Guidance not to disclose personally identifiable information such as sex, age, and nationality and guidance not to publicly disclose any locations for which all potential contacts have been identified through other means (June 30, 2020).

23. The National Human Rights Commission of Korea made recommendations to limit the scope of information disclosure to only the information necessary for the prevention of infectious diseases and not to disclose personally identifiable information (March 9, 2020). The Government continually consulted with the National Human Rights Commission of Korea to implement the recommendations (May 27, 2020; June 26, 2020; and July 7, 2020).

24. In addition, the Government issued an official notice to government ministries and related organizations to request safe and secure handling of personal information, asking to thoroughly destroy all pieces of personal information collected for COVID-19 containment once the respective retention period is over (June 11, 2020).

25. As such, even in the first half of 2020, during the early phase of COVID-19 response, the Government repeatedly advised to disclose only information necessary for the purpose of infectious disease prevention in consideration of various factors such as epidemiological analysis, legal requirements, and the protection of the privacy of confirmed patients, in the disclosure of information such as location history of infectious disease patients and contact situations, and to exclude information that can potentially identify individuals in the disclosure.

26. On the note that “concerns related to the collection and processing of sensitive personal information, which can reveal intimate information like a person’s sexual orientation and private relations, remained” in paragraph 49. (a), the Government would like

to confirm that any information related to sexual orientation has not been collected. If, despite the guidance provided, the trace data disclosed were found to be noncompliant with the privacy guidelines from inspections by the Personal Information Protection Commission, the local Government concerned had been notified and advised to make corrections such as by excluding personally identifiable information in the disclosure by KDCA (Korea Disease Control and Prevention Agency).

27. In the middle of 2020, as the unprecedented COVID-19 pandemic continued, the Government and the National Assembly pursued to strengthen the legal basis of privacy protection by revising the relevant statutes.

28. Most of all, the Infectious Disease Control and Prevention Act has been revised to remove the disclosed information without delay whenever it is not directly related to the prevention of infectious diseases or if the information is no longer in need of disclosure due to the fulfilment of its disclosure purpose (September 29, 2020).

29. Accordingly, the Enforcement Decree of the Infectious Disease Control and Prevention Act has been revised to not include the name, gender, age, residence address, etc., when information on the route, means of transportation, medical treatment institutions, and contact persons of infectious diseases was disclosed (December 29, 2020).

30. As the legal basis for personal information protection had been strengthened in the second half of 2020, the standard examples of information disclosure were provided through relevant guidelines.

31. In summary, the Government recognized the importance of privacy protection and has continually issued documents and provided guidelines to local governments since the early stages of the COVID-19 pandemic, while also collaborating with the National Human Rights Commission or the Personal Information Protection Commission, such as by conducting on-site inspections, to ensure that improvements were made.

32. Additional security measures were implemented to further prevent potential technological vulnerabilities in the access, processing, monitoring, and inspection of personal information. Data or documents containing pieces of personal information are handled by authorized personnel only and encryption modules and solutions are used.

V. Protection of Privacy

33. In relation to paragraph 22, schools are not to inspect students' diaries against students' will. Individual schools are to establish and implement alternative ways to minimize the risk of human rights violation. Schools are recommended to change the name and procedures of writing activities (i.e., content of writing) to "express one's thoughts" and/or "writing time" to strengthen students' expressive capability. In case students voluntarily request their wish to not publicly open their own writing, they can use various ways to express their will such as folding the paper in order to prevent the invasion of privacy.

34. On privacy and children in paragraph 24, the Government would like to inform that, thanks to the amended Enforcement Decree of the Elementary and Secondary Education Act, improvement was made to eliminate elements that may infringe upon student rights by way of broadly stipulating the scope of matters to be specified in school regulations. According to the Enforcement Decree of the Elementary and Secondary Education Act, student representatives and others can participate in a governance committee to share their opinions on enacting and/or amending school charter and regulations as well as students' life in schools.

[Reference - Enforcement Decree of the Elementary and Secondary Education Act]

2019	2021 (Amended Version)
Article 9 (Matters, etc. to be Specified in School Regulations)	Article 9 (Matters, etc. to be Specified in School Regulations)
(1) School regulations (hereinafter referred to as "school regulations") referred to in Article 8 of the Act shall specify the following matters:	(1) School regulations (hereinafter referred to as "school regulations") referred to in Article 8 of the Act shall specify the following matters:
7. Methods of disciplines, other than punishment, appearances, including hair and clothes, examination of personal effects necessary for educational purposes, use of electronic devices, including mobile phones,	7. Methods of disciplines for educational purposes,

35. Regarding the LGBTI rights in the Armed Forces in paragraph 31, pointing out that there had been members of the armed forces questioned by investigators about their sexual orientation and sex life, the Government would like to make it clear that the investigation has been reviewed by the National Human Rights Commission and the result of the review did not include that there was a violation of human rights by threat or intimidation.

36. In the meantime, the Commission recommended that the Ministry of National Defense (MND) be mindful not to humiliate any suspect or violate his/her right to privacy and freedom, including by subjecting them to questionings on matters that are of no direct concern of the facts of suspicion.

37. The Government also ensures conditions for protecting the human rights of soldiers in the barracks regardless of their sexual orientation and allowing them to conduct their military service with other soldiers, in accordance with the Directive on Unit Management, prohibiting any physical abuse, malpractice, insult, verbal abuse, sexual harassment, sexual violence and others against LGBTIs.

38. The Directive stipulates that the abovementioned cases shall immediately be reported and those who committed them are strictly punished, and it also specifies that the commanders shall include the "protection of human rights of LGBTIs" in the education programs on human rights for soldiers.

39. The indecent act stipulated in the Military Criminal Act, however, should continue to be criminalized, as it is to maintain the sound living of the military community and military discipline. The Constitutional Court also ruled that it is constitutional (Constitutional Court Decision 2001Hun-Ba20 decided on June 27, 2002; Constitutional Court Decision 2008Hun-Ka21 decided on March 31, 2011; Constitutional Court Decision 2012Hun-Ba258 decided on July 28, 2016).

40. Another case on the constitutionality of the crime of indecent act in the Military Criminal Act is currently pending in the Constitutional Court, and the MDN will take appropriate measures in accordance with the decision of the Constitutional Court.

41. With regard to paragraph 33 which raised issues on the Smart City projects in Jeju and their impacts on the right to privacy, the Government would like to reiterate that the collection of data by the Jeju Provincial Government using smart city public services and drones is only being conducted with legal measures under the Personal Information Protection Act and its Enforcement Decree.

42. Even though there are no violations under the existing domestic law, the Jeju Provincial Government has taken additional measures to further protect personal information and to prevent any possible infringement of privacy as follows:

- (a) Announcing an administrative notice on drone operation to protect personal information and prevent infringement of privacy;
- (b) Organizing meetings with responsible technicians to reaffirm their resolve towards the safety, security, and protection of privacy regarding drone operation;
- (c) Raising awareness of the matter of privacy by displaying standing signboards, banners, and distributing press releases; and
- (d) Blurring data images including figures or features that identify a certain individual, in order to prevent any infringement of portrait rights.

43. Regarding the right to privacy in the workplace stated in paragraphs 39 and 40, the Government is amending the Data Protection Guidelines (Human relations/Labor section), in light of the National Human Rights Commission of Korea's recommendations on improving systems to prevent the monitoring of workers through electronic devices.

44. The Government, however, would like to clarify that a ban on workplace harassment under the Labor Standards Act, mentioned in paragraph 40, is not related to the abovementioned recommendations by the National Human Rights Commission of Korea but was introduced by the Government's own decision.

45. The Government has made sustained efforts to appropriately use visual data in conformity with the purpose of the Data Protection Act and Article 20 of the Act on the Promotion of Employees' Participation and Cooperation stipulating that matters regarding the installation of surveillance equipment for workers within the workplace shall require consultation by a council.

46. Lastly, in relation to paragraph 62 on requests for metadata, the Government would like to inform that the issuance of warrant is not required even in many other countries when personal information considered non-sensitive metadata is provided to the police and intelligence services.

47. Requiring the issuance of warrant for simple and non-sensitive personal information can lead to delay in crime investigation or flight of the suspect and, therefore, one should consider carefully before recommending the warrant issuance requirement.

48. Also, it is difficult to say that the number of requests for metadata is unreasonably high, considering that telecommunication-related investigations are necessary to conduct criminal investigations with the development of telecommunication technologies, and the requests are mostly for basic data such as phone number or personal information only necessary to identify a person. In addition, there are multiple victims involved in a single crime, which in return inevitably increases the total number of inquiries due to reduplicated cases.

49. The Government would like to confirm that the access to information by the police is strictly managed, as it is obligated to gain approval from the chief of police in written form in order to access information.

VI. Conclusion

50. In conclusion, the Government would like to reassure the SR of its continuous support for his mandate and wishes to thank the SR for the report on his mission to the ROK.

/END/