**Position Paper:**

Country: South Korea

Topic: The Right To Privacy In The Digital Age

Delegate Name: Annanya Lexmi . M

School Name: Adarsh Vidya Kendra

***Country Introduction***:

South Korea is generally considered to be one of the safest countries in the world. The crime rate in 2017 was less than 0.60%. People can roam around at 2 am without fear of life. The same safety extends to the internet as well. According to the International Association of Privacy Professionals, South Korea has some of the world's strictest privacy laws.

The Personal Information Protection Act (PIPA) is South Korea's primary privacy law. It gives South Koreans control over how their personal information is collected and used. For example, companies must explain what data they will collect, what they intend to do with it, and for how long they will use the data. Most importantly, people have the right to have their personal data deleted.

***Cause:***

Honorable Head Table, as a Delegate of the Republic of South Korea under the committee of UNHRC (United Nations Humans Rights Committee), I would like to discuss the lack of cybersecurity despite my country's advancement in the digital world. While there are various rules and regulations to guide people about online safety, taking digital protection into one's own hands is far more effective in South Korea. Also, the government maintains considerable censorship to protect itself from the cyber threat posed by North Korea. So much so, to the point where it can be considered as limiting free speech. The government meticulously watches the browsing behavior of its citizens, including Facebook and Google activities.

***Current Policy:***

In January this year, the Korean Assembly amended three of its major data privacy laws: The Personal Information Protection Act, The Network Act, and The Credit Information Act. Some of the changes include clarifying the concept of personal data, strengthening the Korean Communication Office, and protecting personal data in the finance sector.

***Problem:***

While South Korea takes extensive measures to protect its personal data, the government heavily censors and peeps into its own citizens' digital history. This year, to control the coronavirus pandemic, the government has collected its citizens' personally identifiable data, including tracking their cell phone data, credit card histories, location history, etc. While PIPA requires this data to be deleted after its purpose is served, the government admitted to keeping data from a previous virus epidemic.

The problem is such data can be misused. In fact, internet-related sexual abuse is also a concern in the country. On the 26th of November this year, in Seoul, Cho – Ju Bin was arrested for distributing sexually abusive content that he created by luring and threatening many victims. He ran the Nth Room, a chat room on the encrypted messaging service, Telegram, using private information – sometimes collected illegally from local government offices to blackmail dozens of women and children into performing sexually explicit acts on camera, with thousands of users paying cryptocurrency to watch.

At least 74 women, including 16 teenagers, were trapped in what authorities called "virtual enslavement. Even though he is sentenced to four decades for the crime, cybercrime in Korea happens often.

***Solution:***

The government can coordinate with international agencies to ensure better cybersecurity standards. It should take up diplomacy to build relationships with international countries and ensure cooperation in cybersecurity. Problems like Nth Room should be given worldwide coverage to increase discussion in the public platform.