Forum: Human Rights Council

Issue: Addressing Human Rights Violations in Digital Surveillance Practices in South Korea: Protecting Privacy, Preventing Abuse, and Ensuring Accountability

Student Officer: Omar AbdulHameed

Position: Deputy Chair

Introduction

During the past years, South Korea has faced a severe infringement of rights specifically within the demographic of females that have been abused online through breaching of privacy and the creation of deepfakes. South Korea has faced tremendous technological advancements where technology is responsible for 13% of the GDP and where the total production of the technological industry has been increasing by 5.1% annually. Within South Korea survivors of harassment have been seen as insignificant, shameful and unimportant. South Korea has historically been subject to a patriarchal society with the government being negligent towards gender based crimes, and harassment offenders, leading to widespread abuse where 98% of all domestic abuse victims were women. These two factors have led to many digital crimes, 80% of which victims were women and 98% were seen to be led by men. Women who seek police help are commonly retraumatized or ridiculed, all of which occur on the backdrop of South Korea's patriarchal society, where there is an evident 31% gender pay gap for women and where only 13% of women are board members.

South Korea has been proactive in addressing cybersecurity crimes through imposing harsh legislations and a firm legal framework. South Korea has altered the Information and Communication Network Act where it is imperative that reports on cyber crimes are provided within the initial 24 hours and that noncompliance with authorities will lead to a fine of $21,900. By imposing these harsh measures towards cybercrime offenders, South Korea has taken a step forward to ensure offender accountability and recognition. South Korea is further enforced by more legislation, namely the Personal Information Protection Act, in 2011, which encourages security measures for public and private organisations. Another legislation that enforces measures against cyber crimes would be the Act on Promotion of Information and Communications Network Utilization and Information Protection, imposing the necessity of safeguarding personal information and minimising risks associated with cybercrimes. The Korean Internet and Security Agency (KISA) along with the National Cyber Security Center (NCSC), which work cordially with the South Korean government to minimise the frequency of cybercrimes and increase accountability of offenders.

South Korea has rapidly advanced the idea of maintaining digital privacy within its users through enforcing strict guidelines on digital privacy, namely, the forefront of these policies has been the Personal Information Protection Act (PIPA), which outlines the key principles and rights of all individuals and organizations. The strict legislations established by PIPA are supposed to be imperative within each organisation and thoroughly implemented, non-compliance to PIPA will result in severe repercussions such as fines. However, these policies, such as PIPA, are not educated to all individuals posing a threat, as they may not know their rights.

Definition of Key Terms

AI

A computer system with a special feature involving human-like thinking skills/ abilities. Achieved by taking in a huge mass of data to process. Along with learning from past attempts/ experiences to make the experience better in the future.

Deepfakes

The usage of manipulating AI to alter people's faces to produce images of fake events.

Surveillance

Surveillance is the monitoring of someone's behaviour, activities and information for the purpose of gathering information for the purpose of informing, gathering or influencing.

Personal Information Protection Act (PIPA)

The Personal Information Protection Act (PIPA) was established on 2011 September 30th, later being amended on 4th February 2020 and then on 27 February 2023, it delineates the repercussions, rights, limitations and obligations individuals and organisations have to personal data.

World Cybercrime Index

It identifies and ranks 93 countries based on the frequency and severity of cybercrimes occurring within the area as well as marking specific regions where cybercrimes are especially high.

Korean Internet and Security Agency (KISA)

The Korean Internet and Security Agency (KISA), was founded in 2009 and has been established to promote cybersecurity as well as strengthening the capabilities of cyber security in Korea.

National Cyber Security Center (NCSC)

The National Cyber Security Center (NCSC) in South Korea is a government organisation that has authority over communications technology in the country and is responsible for cybersecurity capabilities and cybersecurity inspections.

Digital transparency

Digital Transparency refers to the clarity and openness of organizations on the internet and the information within said organizations.

Digital censorship

Digital Censorship refers to the legal control or suppression of data on the internet, restricting what the public can view, interact and publish.

Background Information

An Overview of Historical Context

South Korea has been a nation situated on the forefront of technological advancements and development. South Korea has ranked second in the International Innovation Index and has, in the past, has ranked first in the UN e-government survey in 2010, 2012 and 2014. This was subsequent to the rapid industrialization of the Information and Communications sector implementing many high speed network infrastructures in a short time frame. South Korea has seen an immense 13% of its GDP being attributed to technology and the production sector annually increases by 5.1% denoting a rapid shift in many aspects of government and organizations. The South Korean government has consistently allocated resources to the development of its e-government and has received worldwide commendation and acknowledgement. The legislations placed by authorities on technological advancements were adamant and received minor opposition from other parties.

Kim Young-sam Administration (1993-1997)

The Kim Young-sam administration was implemented under the order of President Kim Young-sam, who promoted a more reconstituted government as opposed to the previous years of military oppression and dictatorship. Upon the wake of the new, democratic 'Civilian government', the Kim Young-sam government had instituted the Ministry of Information and Communication as well as implementing the Framework Act of Informatization and formed the Informatization Promotion Committee. The Kim Young-sam government later pushed forward the promotion of high speed network and communications technology, and heavily resourced the idea of implementing technology into many other sectors. President Kim Young-sam had presided over the initial conference of the First Informatization Promotion Expansion report conference and had further impelled the nation to become more fostered in technology within the 21st century.

Kim Dae-jung Administration (1998-2002)

Kim Dae-jung had taken office and had become president during the East Asian economic crisis in late 1997, where during his tenure had focussed on shifting more importance towards an e-government to restructure financial and labour reform within the country. The e-government policy was initially proposed during President Kim Dae-jung's tenure and had opted for a more interconnected government built on the cornerstones of high-speed information and communication. President Kim Dae-jung had promoted digital transparency throughout his time as president and believed it would reduce national competitiveness and corruption. The e-government was instituted during July 1 2001 and had been promoted to being a presidential agenda fostering the allocated time, money and usage.

Roh Moo-hyun Administration (2003-2007)

The Roh Moo-hyun administration is accountable for the majority of technological advancements in South Korea that we see today, having expressed great interest in an e-government and the development of the technological sector. President Roo Moo-hyun had personally led technological projects developing numerous legislations and policies. The Presidential Committee on Government Innovation and Decentralization (PCGID) was formed under President Roh Moo-hyun and developing the technological sector and the e-government was to be articulated in the presidential agenda for the next 5 years. Roh Moo-hyun had heavily publicised and promoted the e-government sustainably throughout many meetings and conferences, to the extent that he had invested USD 850 million into the 31 e-government projects over the next 5 years. In 2004 President Roh Moo-hyun had developed the management systems of the government, the ministry of government administration and home affairs. In 2005 the The Presidential Committee on Government Innovation and Decentralization (PCGID) had been disbanded and was replaced by the e-government special committee which had been more advanced and recognised as well as being more publicised and promoted in South Korea. Overall, the e-government saw great advancement in structure following President Roh Moo-hyun's career through publication and promotion of the technological sector.

Lee Myung-bak Administration (2008-2012)

Once Lee Myung-bak had become president he had shifted the government back to a conservative government. President Lee Myung-bak had limited the usage of an e-government and had significantly reduced the usage of technology and opted for more business-friendly policies. President Lee Myung-bak had significantly regressed the usage of technology particularly by limiting the usage of e-government, no longer part of the presidential agenda, and diminished ICT and informatization.

Park Geun-hye Administration (20013-2017)

The Park Geun-hye administration reversed the effects of Lee Myung-bak to an extent, President Park Geun-hye had personally altered some of the principles that Lee Myung-bak had put in place, such as the information policy, which was transferred to the Ministry of Science, Art, ICT, Future Planning and e-government. Within the newly reinstated policies and e-government, the Park Geun-hye administration had focused on job creation within the technological center.

Challenges to Digital Rights

South Korea has faced varied limitations and challenges in the aspect of digital rights, through aspects such as censorship, traditional views, government regulations and technological advancements. These limitations have been previously addressed and legal solutions have had an impact to an extent, although the existence of these challenges are still noticeable. To maintain strong opinions on legislations and new ideologies such as the e-government it is vital that consistent and strong promotion, publication and funding of these ideas are there as well as have direct interest from the majority of parties. The absence of this will create strict censorship, a lack of rights and distrust.

Freedom of Speech

Freedom of speech is primarily denoted within Article 21 of the South Korean constitution which establishes the right to express one's thoughts freely in public discourse. This Article, though, is still with limitations to balance freedom of speech and public security. An example of this would be the Telecommunications Business Act which mandates the information spread throughout social media to mitigate the prevalence of hate speech and misinformation, likewise, the Criminal Act establishes a concise and intricate legal structure that prevents defamation and false information to preserve the harmony and integrity of society.

Censorship

The primary body deemed to be responsible for the censorship of media is the KCSC, with its primary duty to review media and ensure it to be to the established standards, where if not the KCSC will alter the media in compliance to these rules. The government may also have legal authority to remove posts that they deem to be inciting hate speech, misinformation or violence. The government justifies the usage of censorship in order to preserve and maintain societal integrity, the government is intensely stringent on hate crimes under the Framework Act on Gender Equality (2014) which censors specific hate crimes of certain demographics. The national security law prohibits any recognition of the North Korean regime and is strictly prohibited, with many repercussions.

Data Privacy

Data privacy in Korea is seemingly mandated through the PIPA act which regulates the rights to all data privacy of all demographics and organisations, the authorities responsible for data protection are the Personal Information Protection Committee (PIPC) and the Korean Communications Commission (KCC). There is not any act which regulates privacy of Artificial Intelligence (AI). PIPA and many other data protection legislations align itself with the EU's General Data Protection Regulation (GDPR). The PIPC itself has been elevated to a central enforcement authority where data theft and defamation will be seen as punishable offences with harsh repercussions.

Surveillance

South Korea's extensive past under a military dictatorship, oversaw extensive efforts on surveillance for the purpose of monitoring individuals and suppression. Although a democratic government has been in South Korea, the onset of surveillance still is evident in various forms. During the COVID-19 pandemic, to track infected individuals, the South Korean government began to employ extensive methods of surveillance to monitor the behaviour of individuals. The surveilling was viewed as extreme when the government began tracking movements and transactions, which were seen, by the public, as a breach of their privacy. This depicts the limitations the government faces between privacy and security.

Preventing Abuse

In the past few years, South Korea has been stringent on preventing abuse, especially within the context of an interconnected society. Cyberbullying, is a key factor that the legal framework focuses on, within South Korea, teenagers are 2.85 times more likely to commit suicide compared to adults and adolescents that were bullied are 3.05 times more likely to commit suicide than adolescents that werent bullied. Moreover, South Korea has begun implementing AI to flag down and delete harmful or violent content with many public platforms adopting stricter regulations and policies. South Korea has also passed the Nth Room Prevention Act, which mandates operators to report any malicious behaviour that may occur, such as defamation, blackmail and abuse.

Major Countries and Organizations Involved

Personal Information Protection Commission (PIPC)

Established on September 30th 2011 PIPC was tasked with protecting the nations rights to personal information and the security of it, by creating and enforcing harsh legal frameworks. These legislations were included in the three year 'Personal Information Protection Master Plan', from 2021 to 2023, leading to the advancement in South Korea's data security and digital rights. The PIPC aims to expand its influence internationally, by preeminently diversifying their reach to global public and private organizations as well as increase inspections on public institutions.

Korean Communications Commission (KCC)

The KCC is South Korea's primary body for overseeing broadcasting and telecommunications. The KCC was inaugurated in 2008 under the *Establishment and Operation of the Korea Communications Commission*, taking on more liability from the Ministry of Information and Communication to ensure transparency and security. The KCC's responsibility lies in the security of all users on the internet, the public promotion of data and cyber security and the guarantee of cybersecurity. Since 2008 the KCC has become pivotal in shaping South Korea's digital future having developed appropriate cybersecurity according to the rapid technological advancements.

Korean Internet and Security Agency (KISA)

The KISA was organised in 2009 following a merger between the pivotal organisations, the National Internet Development Agency (NIDA), the Korean Information Security Agency and the Korean IT International Cooperation Agency, tasked with accountability of improving cybersecurity as well as promoting awareness of digital threats. KISA has also sparked major advances for digital security globally through programs such as the Global Cybersecurity Center for Development (GCCD), advancing cybersecurity in Oman, Tanzania, Indonesia and Costa Rica.

Korean Communications Commission (KCC)

The KCC is the primary regulatory authority for all digital broadcasting and telecommunications within South Korea, the KCC was established in 2008 following the restructuring of the Ministry of Information and Communication, the KCC has been involved in many regulations and protections of rights between organisations and individuals. The KCC has also been responsible for the development of many emerging technologies such as Artificial Intelligence (AI), blockchains and the Internet of Things (IoT). The KCC has also pursued global digital security, through organisations such as the International Telecommunication Union (ITU) and cross-border initiatives.

National Human Rights Commision of Korea (NHRCK)

The NHRCK is an independent organization in South Korea that envelopes a large spectrum of human rights, including significant efforts towards the digital rights in South Korea. The NHRCK has been involved with the development of many legal frameworks to align them with global standards and have held many educational campaigns to raise awareness. The NHRCK has also addressed many issues linked with privacy and security, having admonished the mass surveillance practices South Korea had implemented during the COVID-19 pandemic.

Asia Pacific Privacy Authorities (APPA)

The APPA is a network of data and privacy protection authorities, established in 1992, serving as an organisation for relevant government authorities and non governmental organizations (NGO) to collaborate. APPA has consistently established efforts to combat digital rights violations and strengthen security. The PIPC and KISA have consistently been a part of APPA forums and meetings, emphasising cross border data privacy and the effects of the PIPA act.

Timeline of Events

Date	Description of Event
February 5th, 2003	The PCGID was created to oversee the government's advancements in technology
February 29th, 2008	The KCC has been officially established as South Korea's primary body for the regulation of broadcasting and media.
July 23rd, 2009	The KISA was created through the combination of three organizations, namely the Korea Information Security Agency,

	the National Internet Development Agency and the Korea IT International Cooperation Agency to ensure cybersecurity and protect digital rights.
July 2010	Korea had ranked first in the UN e-government survey
March 29th 2011	The PIPA of South Korea was approved by the National Assembly
September 30th, 2011	The PIPA of South Korea came into effect
September 30th, 2011	The PIPC was launched with the aim of ensuring data privacy and rights.

Relevant UN Treaties and Events

- International Covenant on Civil and Political Rights, 23 March 1976 **2200A (XXI)**
- The Right to Privacy in the Digital Age, 18 December 2013 **68/167**
- Promotion, Protection and Enjoyment of Human Rights on the Internet, 1 July 2016 **32/13**
- Universal Declaration of Human Rights, 10 December 1948 **217A (III)**

Previous Attempts to solve the Issue

The establishment of the PIPA in 2011 helped with the prevention of data misuse and regulated the access and collection of data within organisations as well as privatizing personal data more.

National campaigns against online harassment such as ‘Delete the Children campaigns’, to protect the identity of children online and many more campaigns launched to reduce the prevalence of digital crimes and increase awareness to the public.

South Korea’s Ministry of Science and IT has released a cybersecurity master plan that includes enhancing core cybersecurity infrastructure and accentuating the response time and diagnosis for all victims, as well as articulating collaboration with the KISA and other government organizations.

Strengthening government authorities such as the National Intelligence Service in 2015 to increase the capability of these authorities due to combat the increased frequency and magnitude of digital crimes.

The establishment of the e-government initiative to ensure secure data handling within public services, and that further data security is imperative through data protective measures such as encrypted data transmissions, secure authentication systems and data anonymization

. Collaboration between the government and private sector to ensure data security was established in 2013 when the KISA had partnered with many private tech firms to develop cybersecurity measures to reduce the potency of cyber attacks on public technological infrastructure.

Possible Solutions

Have all individuals go through a training course on the importance of digital rights and cyber security to increase awareness amongst the public and reduce the vulnerability of organisations to digital threats.

Establish transparency between individuals and organisations that handle their private data and transparency between organisations and governments authorities to maintain data security of all individuals and limit any misuse by the government.

Establish an ethics committee to oversee all ethical judgement in data handling processes, involving overlooking all algorithms and policies to eliminate all bias.

Guiding Questions

1. What are the long term issues associated with over restriction of data?
2. How does this affect your delegation?
3. How have certain legislations developed over time?
4. How will increased digital security affect the digital economy in South Korea?

5. How significant is the PIPA to only security in South Korea?
6. How significant are NGO such as OpenNet Korea?
7. How strictly will individuals and organisations adhere to these guidelines?
8. What is the significance of the KCC and the PIPC

Bibliography

"World Report 2024: Rights Trends in South Korea." *Human Rights Watch*, 11 Jan. 2024, www.hrw.org/world-report/2024/country-chapters/south-korea.

Kamal, Author Jawana. "A Culture of Shame and Regret: Exploring the Rise of Digital Sex Crimes in South Korea." *UAB Institute for Human Rights Blog*, 6 Nov. 2024, sites.uab.edu/humanrights/2024/11/06/a-culture-of-shame-and-regret-exploring-the-rise-of-digital-sex-crimes-in-south-korea/#:~:text=Digital%20sex%20crimes%20are%20characterized,common%20mechanism%20for%20such%20offenses.

"Covid-19 and the Right to Privacy: An Analysis of South Korean Experiences." *Association for Progressive Communications*, www.apc.org/en/pubs/covid-19-and-right-privacy-analysis-south-korean-experiences. Accessed 26 Dec. 2024.

Johnleenknews. "South Korea's Cybersecurity Law Revisions May Be Too Little Too Late." *KOREA PRO*, 13 Aug. 2024, koreapro.org/2024/08/south-koreas-cybersecurity-law-revisions-may-be-too-little-too-late/.

Intelligence, Generis Legal. "An Overview of Cybersecurity Regulations in South Korea: Security Measures, Reporting Obligations, and Penalties." *Generis Global Legal Services*, 20 Nov. 2024, generisonline.com/an-overview-of-cybersecurity-regulations-in-south-korea-security-measures-reporting-obligations-and-penalties/.

Intelligence, Generis Legal. "Data Protection and Privacy Laws in South Korea: Rights, Obligations, and Standards." *Generis Global Legal Services*, 20 Nov. 2024, generisonline.com/data-protection-and-privacy-laws-in-south-korea-rights-obligations-and-standards/.

"South Korea Data Protection Law (PIPA): Everything You Need to Know." *Didomi*, www.didomi.io/blog/south-korea-pipa-everything-you-need-to-know. Accessed 27 Dec. 2024.

Gositus, www.gositus.com. "Korea Internet AMD Security Agency (KISA)." *AKCF - ASEAN Korea Cooperation Fund*, www.aseanrokfund.com/our-partners/korea-internet-amd-security-agency-kisa. Accessed 27 Dec. 2024.

Chung, Choong-Sik, et al. "Analysis of Digital Governance Transition in South Korea: Focusing on the Leadership of the President for Government Innovation." *MDPI*, Multidisciplinary Digital Publishing Institute, 4 Jan. 2022, www.mdpi.com/2199-8531/8/1/2.

Intelligence, Generis Legal. "An Overview of Freedom of Speech and Censorship Laws in South Korea." *Generis Global Legal Services*, 20 Nov. 2024, generisonline.com/an-overview-of-freedom-of-speech-and-censorship-laws-in-south-korea/.

Ryoo, Kwang Hyun, et al. "Data Protection Laws and Regulations Report 2024 Korea." *International Comparative Legal Guides International Business Reports*, Global Legal Group, 31 July 2024, iclg.com/practice-areas/data-protection-laws-and-regulations/korea.

Kang, Alyssa. "Suicide among Adolescents in South Korea." *Ballard Brief*, Ballard Brief, 6 June 2024, ballardbrief.byu.edu/issue-briefs/suicide-among-adolescents-in-south-korea.

"South Korean Personal Information Protection Commission Announces Three-Year Data Protection Policy Plan." *Future of Privacy Forum*, fpf.org/blog/south-korean-personal-information-protection-commission-announces-three-year-data-protection-policy-plan/. Accessed 27 Dec. 2024.

Appendix or Appendices

Below are useful links that will help develop your understanding on the issue of digital rights in South Korea

For Example:

I.

https://generisonline.com/an-overview-of-cybersecurity-regulations-in-south-korea-security-measures-reporting-obligations-and-penalties/ (South Korea's Cyber security measures, obligations and penalties)

This website is useful as it articulates all the necessary measures the government has implemented as well as how harsh the penalties are providing an understanding on the prevalence of this issue.

II.

https://www.mdpi.com/2199-8531/8/1/2 (How change in South korea's government has caused technological innovation)

This website is useful because it showcases how change within the government has caused the technological sector to grow including policies such as PIPA, KCC, KISA and the e-government.

III.

https://generisonline.com/an-overview-of-freedom-of-speech-and-censorship-laws-in-south-korea/ (Censorship in South Korea)

This website is useful because it shows the legal structure around freedom of speech and censorship in South Korea and the penalties and impacts of these legislations.

IV.

https://www.apc.org/en/pubs/covid-19-and-right-privacy-analysis-south-korean-experiences (The harsh security measures South Korea used during COVID-19)

This website is useful as it implores the harsh regulations that South Korea had set for COVID 19 and how the government had invaded the privacy of many individuals without their permission.

To end on a very important note: plagiarism will **NOT** be tolerated at MUN@NIA V; there is no need to elaborate on this point.