# South Korea IGF Report 2020


KIGA
다자간인터넷거버넌스협의회
Korea Internet Governance Alliance

KrIGF
한국인터넷거버넌스포럼
KOREA INTERNET GOVERNANCE FORUM

**Introduction of Kr-IGF**

At the World Summit on the Information Society (WSIS) meeting held in 2005 in Tunisia, *Tunis Agenda has* recognized the need for a broad based discussion of public policy issues relating to the Internet. Ever since then Internet Governance Forum (IGF) has been providing a platform locally and globally for discussions. IGF bring various stakeholder groups to the table as equals to exchange information and share good practices.

While the IGF may not have decision-making mandates, it facilitates a common understanding of how to maximize Internet opportunities and address risks and challenges. In the meantime, IGF is increasingly being expected to produce more specific outcomes like 'recommendations' on internet-related policy issues. In 2014, the NET Mundial, the Global Multistakeholder Meeting on the Future of Internet Governance, was held in Sao Paulo, Brazil. The statement of NET Mundial affirmed the need for a strengthened IGF's role.

South Korea's Internet Governance Forum(Kr-IGF) provides a open forum to inspire those with policy-making power in both the public and private sectors, Kr-IGF has been activated since 2012. From 2017, we begun to publish final report both in Korean and English. Kr-IGF has been recognized as a member of IGF National and Regional IGF initiatives (NRIs) by Secretariat of the United Nations Internet Governance Forum, and also participating in activities of Asia Pacific Regional Internet Governance Forum (APrIGF).

Kr-IGF is now operated by *Korea Internet Governance Alliance* (KIGA), a coalition of private and public sector. Kr-IGF primarily aims to stimulate policy-discussions among stakeholders from diverse sectors: internet business entrepreneurs, software developers, internet engineers, technical community, start-ups, youth groups, non-profits, civil society activists, media scholars, academics, governmental agencies and public institutions. Like other IGF National and Regional IGF initiatives, Kr-IGF has the non-binding outcome of a bottom-up, open, and participatory process that brings multistakeholders into the dialogue about Internet related policies.

**Theme, Venue, and Date**

Due to the global coronavirus (COVID 19) outbreak, South Korea Internet Governance Forum's 2020 conference went virtual. Kr-IGF program consisted of three tracks of workshops, two tutorials and one open consultation session. The entire Kr-IGF sessions were openly accessible and live stream has been broadcast on Youtube. In Kr-IGF event, participants have opportunities to discuss and make comments on policy questions pertaining cutting-edge technologies and internet.

- When : Aug.21 Fri 2020, 10 am ~ 6pm
- Online Access
  - Kr-IGF website : http://www.krigf.kr
  - YouTube Live Stream: http://www.krigf-channel.kr
  - Social Media : http://facebook.com/krigf.kr/
- Host : The Korea Internet Governance Alliance (KIGA)
- Co-organizers: The Korea Internet Corporations Association, Gabia, Korea Hosting Domain Association(KHADA), The Future of Internet Forum, Korea Information Society Development Institute (KISDI), KT GiGA Genie, Naver, Kakao Corp., Hankyul Law Group LLP, Barun Law LLC, GP3Korea, Open Net Korea, Korean Progressive Network (Jinbonet), Institute for Digital Rights, and Korea Internet & Security Agency (KISA)
- Funding : Ministry of Science and ICT, Kakao Corp., Naver, Gabia, and KT GiGA

Genie

- Contact: KrIGF Secretariat krigf@kiga.or.kr
  Eun Chang Choi eunchang.choi@aya.yale.edu

**Key Discussion Areas**

The Kr-IGF conference in 2020 consisted of two tutorials and eight workshops that provided three thematic sub-tracks *Security, Connectivity* and *Youth.*

*Tracks*

- Track I ***Security*** discussed about i) the definition of pseudonymized data for scientific research with regard to the revised Korean Personal Privacy Protection Act as of 2020, ii) approaches to safer Internet countering sexist hate speech and discrimination, and iii) digital tracing practices for COVID-19 seeking a balance between public health and personal privacy with a comperative perspective.
- Track II ***Connectivity*** covered issues regarding i) information governance of data from smart cities, ii) the criteria for network interconnection fee under 'net neutrality rules'
- Track III ***Youth*** focused on i) empowerment of women in informatics engineers, ii) personal data disclosure affecting info-human rights, iii) underprivileged groups in the untact culture.
- Two tutrotial sessions deepened public understanding of i) the Global landscape of AI Ethics Principles, and ii) Now and the future of Domain Name System (DNS)
- Open consultation session focused on the implication of European General Data Protection Regulation (GDPR) and recently revised Personal Privacy Protection Act as of 2020 in Korea to WHOIS database of Korean domain names (.kr)

**The Features of Kr-IGF 2020**

As the COVID-19 pandemic shaped the human life around the world presenting unprecedented challenges to public health, safety, and works, Kr-IGF program committee decided to focus on the *New Normal* in which *Connectivity*, and *Safety* are regarded as the vital value. Untact social and economic activities heavily depend on internet connectivity. In the face of COVID-19, non face-to-face service has become commonplace. The pandemic increased average daily time spent on smartphone, Over- The-Top streaming video consumption, and changed our way of life. Online education, virtual meetings, remote working, digital media content consumption (social media apps, online games, streaming videos) have been scaling during social distancing. With the rise of concerns over coronavirus infections, the most noticeable changes can be found in the network traffic surge, digital platforms, and on-demand food deliveries.

Against this backdrop, 2020 Kr-IGF looked into how digital technologies can help combat the devastating effects of the pandemic offering nine workshops on three thematic tracks of *Safety*, *Connectivity*, and *Youth*. Several workshops paid keen attention to how to strike a well-balance between public health and personal privacy in information technology–based tracing practice in a way of response to COVID-19 in South Korea. At the same time, we were concerned with issues Internet Address Resources, Domain Name System (DNS), and Artificial Intelligence(AI).

- Kr-IGF workshops brought meaningful inputs on wide range of current issues. For example, the merits of multi-stakeholder based cybersecurity policy-making, curbing the spread of disinformation, and social, ethical, political ramification of data ethics and deployment of artificial intelligence technologies.

- Improved accessibility to KrIGF is noticeable. In the sense of ensuring access to the

disabled and keeping a record, we decided to provide text interpretation at the event. Stenographers dictated workshop scripts on real time basis, so that the text visibility significantly enhanced the accessibility of those who with hearing disabilities. When it comes to text interpretation service, we collaborated with AUD (www.sharetyping.com), a social cooperative.

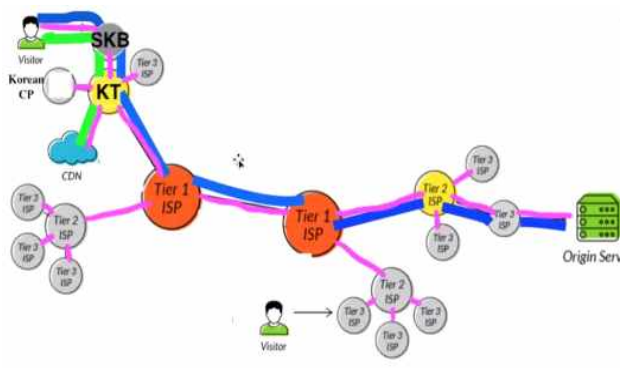
- Secretariat of Kr-IGF has set a Youtube channel and provides archive of video footage. With a fixed URL (www.krigf-channel.kr ) the past annual conferences of Kr-IGF are accessible.

- Panel participations have been remarkably diversified. Panelists and discussants represented internet businesses, start-ups, mobile app developers, computer science engineers, civil rights activists, personal privacy advocates, feminists organizations, political scientists, youth groups, academia, progressive lawyers, National Human Rights Commission (NHRC), civil coalition for economic justice, and Personal Information Protection Commission.

- More importantly, the share of youth group commitment grows to prominence. We have seen the steadily increase of workshop proposals and participation from youth including KIGYS (Korea Internet Governance Youth Stakeholders). They independently organized Youth track workshops inviting panelists from businesses and government sectors. Young volunteers also publicized the event and actively shared their own experience in blog postings.

**Kr-IGF 2020 Photos**

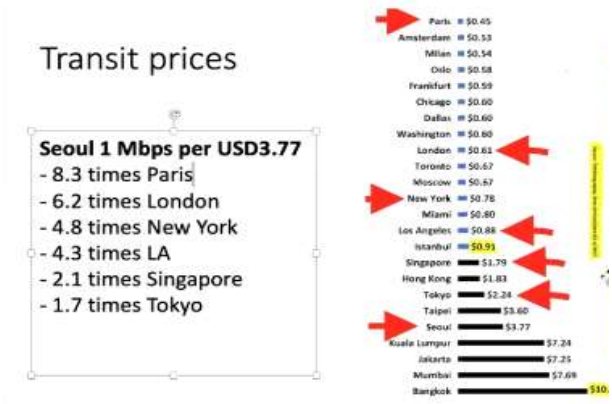
Kim, Seok Hwan (Commissioner, KISA)

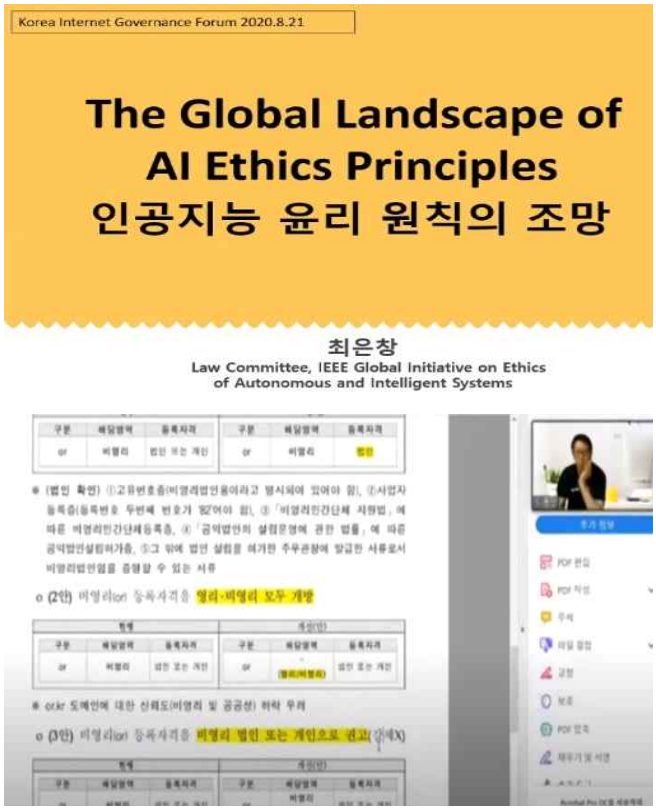




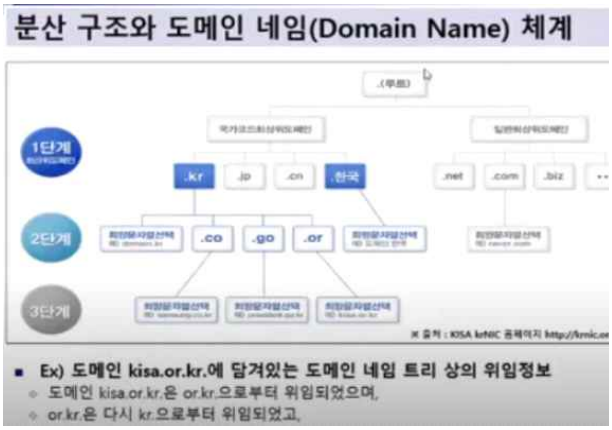

**Kr-IGF YouTube Live Stream and Archive**

URL: www.krigf-channel.kr


Transit prices
Seoul 1 Mbps per USD3.77
- 8.3 times Paris
- 6.2 times London
- 4.8 times New York
- 4.3 times LA
- 2.1 times Singapore
- 1.7 times Tokyo
Paris $0.45
Amsterdam $0.53
Milan $0.54
Oslo $0.58
Frankfurt $0.59
Chicago $0.60
Dallas $0.60
Washington $0.60
London $0.61
Toronto $0.67
Moscow $0.67
New York $0.78
Miami $0.80
Los Angeles $0.88
Istanbul $0.91
Singapore $1.79
Hong Kong $1.83
Tokyo $2.24
Taipei $3.60
Seoul $3.77
Kuala Lumpur $7.24
Jakarta $7.25
Mumbai $7.69
Bangkok

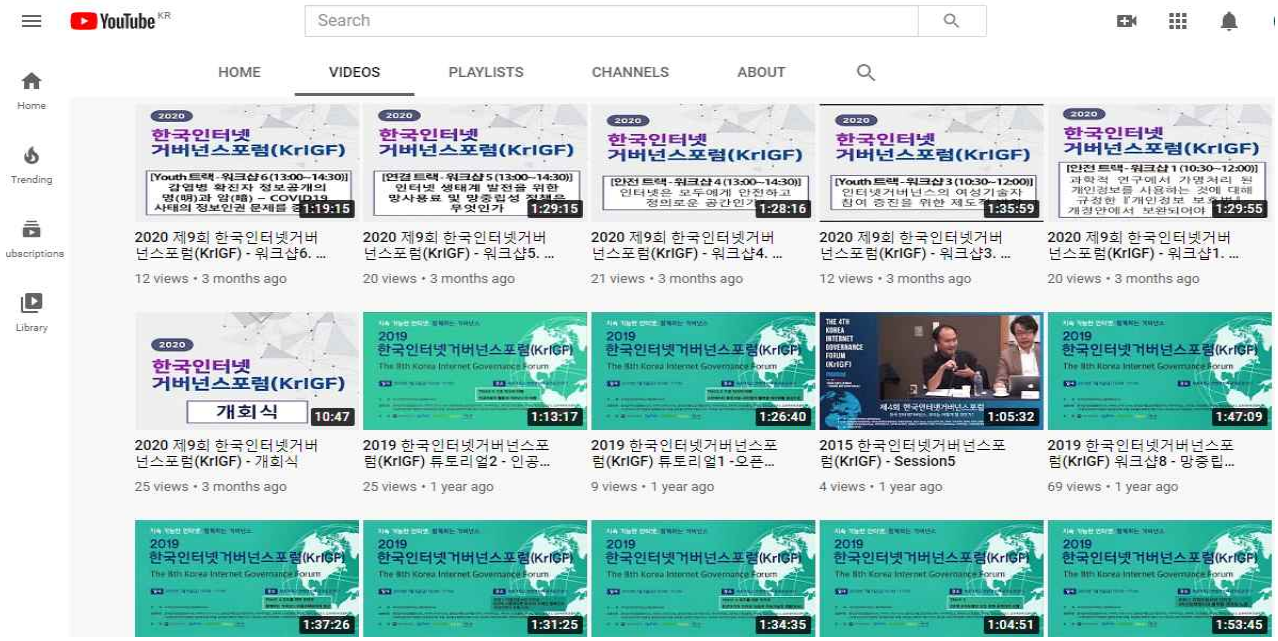

Korea Internet Governance Forum 2020.8.21
The Global Landscape of AI Ethics Principles
인공지능 윤리 원칙의 조망
최은창
Law Committee, IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems


COVID-19 이후의 뉴노멀, 언택트 문화 속의 사회적 소외계층
터넷 이용 여부 및 비이용 원인 : 장애인


분산 구조와 도메인 네임(Domain Name) 체계
1단계
2단계
3단계
.kr
.jp
.cn
.한국
.net
.com
.biz
.co
.go
.or
Ex) 도메인 kisa.or.kr.에 담겨있는 도메인 네임 트리 상의 위임정보
도메인 kisa.or.kr.은 or.kr.으로부터 위임되었으며,
or.kr.은 다시 kr.으로부터 위임되었고,


COVID 19 Contact Tracing Apps 설계방식 2
Centralized contact tracing apps 설계
확진자가 접촉했던 주변 이용자들의 가명 블루투스 ID까지 알수 있음.
Centralized approach


ICT/SW 분야 여성인력 배출 및 고용 비중
한국 여성 ICT/SW 인력 비중
세계 STEM 분야 여성인력 비중




## Kr-IGF 2020 Program Schedule

| | Track 1 | Track 2 | Track 3 |
|---|---|---|---|
| | Safety | Connectivity | Youth |
| | Theme | | |
| 10:00 ~10:30 | Opening Ceremony<br>Moderator : Kim, Tae Eun (Chair, KrIGF Program Committee)<br>Opening address : Lee, Dong Man (Chair, KIGA), Kim, Seok Hwan (Commissioner, KISA)<br>Welcome speech: [Tech community] Kim, Kyoungseok (Pusan Univ),<br>[Public Sector] Kim, Insook (Korea Customer Service), [Civil Society & Youth] Miru (Jinbonet) | | |
| 10:30 ~12:00 (90') | Pseudonymized personal Data for Scientific Research in Personal Information Protection Act | Post COVID-19 and Informational Governance : Smart City's Data by the Green New Deal and the Public Nature of the Digital Platform | Institutional Plan to Increase Participation of Female Engineers In Internet Governance Dialogue |
| | Moderator : Rye, Seoung Kyun (Netflex )<br>Panelists: Kim, Borami (Citizens' Coalition for Economic Justice)<br>Kim, Jae Hwan ( Korea Internet Corporations Association),<br>Hwang, Chang Keun (Hongik Univ)<br>Lee, Wook Jae (Korea Credit Bureau)<br>Lee, Han Seam (Personal Information Protection Commission, PIPC)<br>Seo, Cheawan (MINBYUN , Lawyers for a Democratic Society) | Moderator : Seong, Min Kyu (UNIST )<br>Presenters: Park, Daemin (MBN),<br>Seong, Min Kyu (UNIST)<br>Panelists: Lim, Jongsu(Sejong Univ)<br>Chea, Young Gil (HUFS Univ),<br>Oh, Byong-il (Korean Progresstive Network, Jinbonet) | Moderator : Kim, Tae Eun (KISDI)<br>Presenter : Ko, Eubi (KIGYS)<br>Panelists: Choi, Eun Phil (Kakao Corp) Moon, Soboek (KAIST),<br>Byun, Kyu Hong(Skelter Labs),<br>Jeon, Yojin (Open Tech Lab for Women) |
| 12:00 ~13:00 | Break (Luncheon) | | |
| 13:00 ~14:30 | Is the Internet a Safe and Fair Space for Everyone? | Reasonable Level of Network Usage Fee a nd Network Neutrality Policy for | Disclosure of Infected Patients' Data : Privacy and Human Rights in Public Health Measure of |

| | | | |
|---|---|---|---|
| (90') | | I nternet Ecosystem | COVID-19 |
| | Moderator : Miru (Jinbonet)<br>Presenter: Oh, Kyung Mi (Open Net)<br>Panelists: Lee, Seoung Hyu (The Rainbow After Rain), Oh, Young Teak (NHRC Korea), Yoekbi (Scarlet ChaCha)<br>Yang, Jihea(Wetee) | Moderator : Oh, Byong-il (Jinbonet)<br>Panelists: Kim, Ejun(Kyonghee Univ)<br>Park, Kyoung Shin (Korea Univ)<br>Jeong, Mina (Korea Startups Forum)<br>Shin,Young Woo (National Assembly Research Service) | Moderator : Son, Jaewon (UNDP, KIGYS)<br>Panelists: Hee Woo (Jinbonet)<br>Park, Hanhee (Law of Hope)<br>Lee, Jae Young (DongKuk Univ)<br>Ko, Eubi (Ewha Womans Univ)<br>Lee, Jiwon (Seoul Women's Univ)<br>Lee, Wonsang (Chosun Univ) |
| 14:30 ~14:40 | Short Break | | |
| 14:40 ~16:10 (90') | Request to the Korean Personal Information Protection Committee<br>Moderator :Yoon, Boknam (Hankyul LLP)<br>Presenter: Shim, Woo Min (Gyeongin National Univ of Education)<br>Ko, Whan Kyoung (Lee & Ko LLP );<br>Kim, Jae Hwan ( Korea Internet Corporations Association)<br>Jong, Jeyeon (Consumers Union of Korea), Chang, Yeokyoung (Institute for Digital Rights) | Tutorial<br>: The Global Landscape of AI Ethics Guidelines<br>Presenter: Choi, Eun Chang (The Free Internet Project) | New Normals after COVID-19: Socially Underprivileged in the Untact Culture<br>Moderator : Lee, Jae Young (DongKuk Univ)<br>Presenter: Park, Tae Kyun (Chungnam Univ)<br>Panelists: Kim, Jo Eun (Center for Freedom of Information and Transparent Society)<br>Kim, Dae Won (Kakao Corp)<br>Kim, Chul Whan (Information Culture for the Disabled), Hwang, Sun Young (Ministry of Science and ICT)<br>Janng,Chang Ki (Seoul Science and Technology Univ) |
| 16:10 ~16:20 | Short Break | | |
| 16:20 ~17:50 (90') | ICT-based Tracing in Response to COVID-19 : Striking a Balance Between Public health and Data Privacy<br>Moderator : Choi, Eun Chang (The Free Internet Project)<br>Presenter: Choi, Eun Chang (The Free Internet Project)<br>Choi, Soojeoung (Universität Hamburg, Germany)<br>Panelists: Kimm, Heejin (Yonsei Graduate School of Public Health),<br>Woo, Harin (Seoul Science and Technology Univ)<br>Kim, Eun Soo (Seoul National Univ)<br>Choi, Jea Woo( The Weird Sector) | Tutorial<br>: Now and The Future of Domain Name System (DNS)<br>Presenters:<br>Seok, Wonjin (NS Consulting )<br>Kang, Sang Hyun (Korea Internet & Security Agency) | Open Consultation: WHOIS Domain Privacy Policy under the New Personal Privacy Protection Law of Korea<br>Moderator : Yoon, Boknam (Hankyul LLP)<br>Presenter: Internet Address Resources Team (Korea Internet & Security Agency)<br>Speech and Questions: Virtual attendees from the floor |

## Summary of Kr-IGF 2020 Workshops

### [ Workshop #1 ] Pseudonymized Personal Data for Scientific Research Purpose in Korea Personal Information Protection Act

**Background** With the emergence of sensing technologies, mobile app and IoT, the collection and processing of personal data are getting more extensive. The revised Personal Information Protection Act allows the use of pseudonymized personal information for 'scientific research'. According to the Act, pseudonymized data can be processed regardless of the consent of data subjects on several occasions: statistical purposes, scientific research purposes, and archiving data for public interests. So far, however, the Act does not provide a clear definition what *scientific research* means. Therefore, digital human right activists and lawyers contend that even pseudonymized personal data can be misused or compromised by private companies in the form of commercialized scientific research.

**Policy Questions**

- According to Personal Information Protection Act, what is the scope of scientific research? To what extent could data subject rights be limited for scientific research purposes?
- Would it be a sufficient measure to protect data that the combination of pseudonymized personal data can be carried out by only authorized entities designated by Personal Information Protection Commission (PIPC) or other government authority?
- In pseudonym processing for scientific research purpose under the Personal Information Protection Act, what sort of measures should be followed to minimize the risk of data re-identification?

**Discussion**

- In the strict sense of text interpretation, the scope of 'scientific research' also includes industrial use of data in private sector. The definition widely accommodates technology development and demonstration, basic and applied science by privately invested research agenda. When the industries use it for scientific research purpose, pseudonymization is a measure to guarantee of the safety. We would better focus on how to practice it properly.
- In order to protect the privacy in a use of artificial intelligence technology, biometric data, medical data, various ethical standards are increasingly being strengthened. Scientific research method must meet the standards.
- The pseudonym information is data that is used by lowering the risk of quasi-identifiable data items that can infer an individual without using highly identifiable information at all.
- Critics still worry the possibility that individuals' identity could be compromised through the combination of pseudonymized data with other relevant data from the third party. The potential risk of re-combination should be strictly controlled. It is duly considered by the Act already.
- The Personal Information Protection Act needs complementary legislation. It aimed at the goal of matching the level of protection to the GDPR level, but when the Data 3 Acts passed, the rights of data subjects were not properly discussed. For example, *a right to object to profiling* should be legislated.
- Revised personal privacy protection enacted a provision of burdensome penalty in case of misuse of pseudonymized personal data. In this light, the industries are hesitate to use it because of uncertainty that companies may be at legal risk.
- Establishing robust data security system is essential in using pseudonymized data. But there has been wide-spread anxiety over re-identification as the mechanical combination increases for commercial purpose. Pseudonymized data are being processed for a specific purpose, but re-engineering is subject to prohibition by lasw. Moreover, from businesses standpoint, the industries could hardly find incentive to re-identify pseudonymized data.
- According to the Act, only specialized agencies with technological capacity, designated by the government authority, could precede data combination. The transparency of data use will heavily depend on good practice of data combination and merging process. All in all, the industries intend to use it safely, rather than self-producing combined data.

**[ Workshop #2 ] Post COVID-19 and Informational Governance : Smart City's Data by the "Green New Deal" and the Public Nature of the Digital Platform**

**Background** The manufacturing-based and finance-based governance is over, and now it has shifted to the era of information governance driven by ICT and artificial intelligence. The 'Data 3 Acts' have passed Korean National Assembly in 2019. These Acts allegedly provide the protection of personal data privacy but also promote the use of data for certain purpose without consent. Namely, corporate and market approach to personal data is allowed. In the meantime, the outbreak of coronavirus pandemic calls for new digital governance paradigm. In this regard, it is necessary to rethink whether the governance of the "Green New Deal" policy will effectively deal with COVID 19 crisis.

**Policy Questions**

- Personal data in smart cities are the core resources of the *Green New Deal* project. In this setting, could the smart city function as the central axis of governance ?
- Could the "Green New Deal" project be seen as building robust data governance that can effectively deal with the COVID 19 crisis and underpin the public nature of the digital platform?
- How should the data of smart cities and the public nature of digital platform be redefined in the context of 'information governance and 'post-COVID 19'?
- Could the reinforced Personal Information Protection Commission (PIPC) properly carry out the governance leadership for smart city operation in the post- COVID 19 era?
- Is there the need for a separate, standing governance system (i.e., Public Information Processing Committee) for COVID 19 crisis management?

**Discussion**

- Information commodification should be seen as a change in the governance system in a macroscopic context. The change of governance is that the quantitative transformations of the data and Internet are being replaced by individual lives in society. From this view point, smart city is a good example.
- The revision of Korea's Personal Information Protection Act in 2020 that incurred institutional changes in data use and privacy rights can be understood in terms of reinforcing the neoliberal system. In this respect, the post-CDOVID 19 policy of the "Digital New Deal" policy takes a neo-liberal approach to the privacy of users for data created from digital media use.
- The smart city project has primarily focused on digitalization by converting traffic, parking, crime prevention, disaster prevention, facility management, and administrative services to digital hardware or software. However, the project design and implementation have been led by public administrative agencies. As a consequence, the opportunity and space for civil society participation were relatively lacking.
- The smart city policy emphasizes participation, but as evidenced by many Western case studies of smart city through *Living Lab* have not brought meaningful outcome enhancing local culture/knowledge. Some critics pointed out that the current digital media policy, the "Digital New Deal", centers on juggernaut ICT businesses will be only strengthening the power of capitalism, centralizing administration, and data surveillance system. It would fail to build data governance that can effectively deal with the COVID 19 crisis, and it has no expectation of public nature of the digital platform.

**[ Workshop #3 ] Institutional Plan to Increase Participation of Female Engineers In Internet Governance Dialogue**

**Background** The multistakeholder model of internet governance is the mechanism which reflects diverse stake-holders' views encouraging discussion from many different angles about the technological development and policy-making regarding the internet. The swath of female engineers in computer engineering, such as networks, infrastructure, computer systems, and data analytics, is on the rise. But the voice of female engineers who get involved in internet governance dialogue is still relatively small. Namely, women's view points and opinions have been largely excluded in internet governance discussion while

female engineers have their say on what matters. The purpose of workshop was intended to discuss about the structural problems and the obstacles of lacked females voice, and approach to improve the current situation.

**Policy Questions**

- What caused insufficient participation of females, at least, in the field of computer science in Internet governance dialogue?
- How can we suggest a series of institutional supports and measures to increase female participation?

**Discussion**

- The proportion of female workforce in the science and technology sector is quite low globally. The volume of women's education in the ICT field in South Korea is not that much high. In particular, the female doctoral rate is lower. The number of college graduated female and its employment rate are relatively high. But not in the ICT field.
- Not just in internet governance, but also many other areas, Korean society has not seen much women's participation and voices. In particular, in the technology and engineering fields, female's share is significantly limited. So, the *Open Technology Lab* for Women has been established to improve women's participation in tech fields. Open Technology Lab for Women strived to connect two sectoral concepts: technology and women.
- The gender wage gap in South Korea has been the worst amongst 37 OECD member countries (around 32 %). The proportion of female-led start-ups is just 10% more or less. Moreover, there are few women in the field of data science and artificial intelligence R&D. These structural problems give a difficulty to find women who will be active in internet governance forum.
- One suggestion would be to expand education pipeline from elementary, middle, to high school. That is, for example, if middle schools increase the affinity of SET(Science, Engineering, and Technology) education for female students, then subsequently they will have more probability to choose a career path in ICT, science, and engineering.
- To increase the number of female technicians, accessibility to technological community for women would be important.
- It is socio-culturally important to create a technology-friendly atmosphere for women. The proportion of training more women engineers could increase through the design of institutional choice. In addition, it is essential to create an atmosphere that voluntarily respects diversity.

**[ Workshop #4 ] Is the Internet a Safe and Fair Space for Everyone?**

**Background** Today's cyberspace seems like a 'tilted playground'. Not only that, but the public sphere of internet is being dominated by loud speakers that amplifies and reproduces the hatred, gender discrimination, and propaganda of extreme hostility against minority groups : the disabled, transgenders and sex workers. Through internet mirroring, Korean females were in solidarity with women around the world. The feminist hashtag (#) online movements, which continued from 2015 to the present, has been connected women on a global scale. But the solidarity through the internet, which socially marginalized groups have dreamed, is crumbling. In the meantime, the 'Nth Room' case( n番房 事件) has shaken the society. The criminal case has been deeply involved in blackmail, extortion, sex trafficking, and sexual exploitative video. The operators of Nth Room commercially sold sexual exploitation videos commercially getting subscription fee via Telegram channels. However, someone tolerated this cybersex crime as a play culture and held the victim responsible, not the perpetrator. This workshop invited female activists and an officer of the National Human Rights Commission of Korea.

**Policy Questions**

- What is the reality of hated and exclusion currently faced by transgenders, sex workers, and young females in Korean society?
- What is the "safety" of a cyber space. What kind of excessive expressions have been

used to exclude others, criticize and discriminate against minorities for safety reasons?
- What is needed to make the internet "safe for everyone"?

**Discussion**

- In the case of transgenders, they have been invisible as marginalized group, but they have never been properly respected. Then little by little, the stories of transgenders and LGBTs began to become visible. But the hatred toward transgenders has intensified. Hate speech is occurring in a complex context, and social awareness and supports for transgender is still quite weak in Korean society.
- There is a contradictory gaze toward sex workers. In the male society, sex workers are criminals who make money easily by selling themselves promiscuously. Female activists call for the abolition of prostitution since they devalue sex workers' movements. From the stance on the feminist movement, youth female sex workers are just victims of exploitation. Thus, the experience and voice of youth female sex workers cannot be respected or embodied as a subject with language.
- The National Human Rights Commission of Korea (NHRC) has consistently responded to hate speech and discrimination issues, but it is still insufficient. In practice, the victim must be designated, but it is true that the hate discrimination expression targets vague groups or unidentified individuals. It makes it difficult to handle the case. Having been aware of the practical obstacles the NHRC makes efforts to develop a hate discrimination response plan and publishes hate expression report.
- Once some have experienced cyber bulling, they have to abandon the cyberspace or social media account where they were sharing, communicating, and forming relationships. Suffer from damages, why they leave the digital space? Because it is difficult to track the hate speakers and abusers. Online safety cannot be expected in situations where the abusers cannot be held accountable.
- When it comes to safety, the Youth Protection Act in Korea only has been a tool to regulate youth rather than providing protection. In this situation, female adolescents can only talk about their sexual identity, sexual pleasure, and sexual discourse in a deviant way. So female adolescent sex workers became active on an anonymous basis, longing for a safer space. However, they realized that digital space is also an unsafe space.
- Today's hate expression regulations mainly regulate rough expressions and swear words without context or historical consideration. In the future, it is necessary to share what is hate expression and what contains the context of discrimination based on various experiences. To this end, internet portal companies also have to acknowledge some level of responsibility for encountering hate speeches against transgenders, sex workers, and young females , and should play their own role.

**[ Workshop #5 ] A Reasonable Level of Network Usage Fee and Net Neutrality Policy for Internet Ecosystem**

**Background** Internet traffic has dramatically increased due to the untact culture sparked by social distancing and stay-at- home orders in COVID 19 pandemic. At the same time, a controversy is growing over who should bear the cost and be responsible for stable internet connectivity. In Korea, critics make a case that large overseas Content Providers (CPs)– Google and Netflix– are not properly paying network usage fees to Korean telecommunications carriers. Domestic CPs –Naver and Kakao –have been paying enormous network usage fees. Is this a situation of reverse discrimination? On the other side, some counterargued that Internet Access Services by domestic CPs and Cache Services by foreign CPs are different. So, network usage fees should be calculated differently according to the nature of services. Meanwhile, it is also controversial whether current network neutrality policy should be changed in 5G environment? In the background of arguments regarding network usage fee, different stance of actors are intertwined (i.e., telecommunications

companies, overseas CPs, domestic CPs, small CPs). The government should implement a policy surrounding network usage fees to protect the internet ecosystem and the user's interests.

**Policy Questions**

- Is there reverse discrimination in network usage fees between domestic and overseas Content Providers (CP)?
- Both domestic and overseas CPs complain that network usage fee required by domestic telecommunication companies is higher than that of overseas. Is the Korea's domestic network usage fee (or Internet access fee) reasonable price?
- What should the public policy to resolve the current conflict related to network usage fee?
- 5G networks have network slicing architecture that subdivided into virtual networks. Should network neutrality exceptions be applied to managed services in 5G environments such as autonomous driving and telemedicine?

**Discussion**

- In practice, stable internet service would be difficult without a cache server provided by overseas CPs. While domestic CPs are paying network usage fee, overseas CPs cover the cost of installing/ maintaining huge cache servers (CDN) instead of paying the network usage fee to domestic ISPs. Although some digital content of a CP (ex: YouTube, Netflix) passes through domestic internet networks, it is nothing to do with incurring additional costs. Thus, CPs do not need to pay network usage fee in proportion to the data capacity based on the assumption that it generated the surge of traffic burden.
- A level of network usage fees (*transit price*) in Korea are relatively expensive to compare with other OECD countries. Small start-ups and medium-sized CPs with no bargaining power are struggling to cut the price of network usage fees in negotiation with giant ISPs.
- Network usage fees should be understood as *connection fees* in line with the basic principles of Internet. There is no cost incurred by the data passing through the internet line. Current high level of network usage fees rates are due to the 'caller pay-as-you-go system' from 2016. It is an unreasonable measured rate system and should be abolished.
- Due to the pay-as-you-go system, each ISP tried not to generate heavy traffic above non-chargeable interconnection range (1:1.8 ratio). This structure of the system literally pushed many ISPs to evade conveying killer contents.
- The initial purpose of the 'notification about interconnection between telecommunication facilities' (an administrative fiat proclaimed by Ministry of Science and ICT) was to prevent unnecessary competition between large network operators and medium-sized network operators. It unexpectedly caused a conflict between ISPs and CPs. It is said that while it did not take account of the increased burden of CPs, it is combined with ISP's profit making. According to this rule, if CPs content business flourishes, a level of network usage fees rises proportionately. However, ISPs companies strongly argue that foreign CPs must share the costs for network quality maintenance.
- ISPs argued that hyper sensitive data traffics in 5G need prioritization or differentiation since 5G is complexity network that linked a matter of life and death (ex: remote surgery, driver-less cars). But some critics claimed that the net neutrality principle should be applied in 5G environment as well. In some ways, 5G managed service or network slicing should not affect the general principle of internet. This is part of the European managed service provision, which requires net neutrality.

**[ Workshop #6 ] Disclosure of Infected Patients' Data : Privacy and Human Rights in Public Health Measure of COVID-19**

**Background** South Korea has effectively contained coronavirus outbreaks. The government collected and disclosed some information of confirmed patients and movement

paths of them. It was a part of the K-quarantine measures. It is believed that public warning by informing location, age, gender, residence areas, and travel paths of patients prevent the spread of infection. Partial patients' data without names were released in accordance with the Act on the Prevention and Management of Infectious Diseases. However, some found it uncomfortable since intimate details of COVID-19 cases also were disclosed. In particular, when the details of the sexual minority publicly exposed, their gender identity and sexual orientation were compromised. Subsequently, cyber bullying, assumption of personal identity, and malicious comments for confirmed cases ensued. As can be seen from a survey that citizens are more afraid to be publicly criticized than being infected with the coronavurius itself. Personal data disclosure highly intensified the social stigma that regards coronavirus patients mere as source of pathogen.

**Policy Questions**

- What kind of human rights violations does personal information disclosure cause?
- In public health purpose, was the scope of personal information disclosure appropriate? How to make a balance between the privacy protection and the public interests?
- What human rights protection measure could be done for compromised patients because of information disclosure?

**Discussion**

- Epidemiological investigation authorities are connected with public institutions, private companies to run COVID 19 contract tracing system. This process inevitably requires to gather a lot of personal information. In this way, privacy of individuals can be seriously infringed if there is no strict guideline or limitation.
- The current contract tracing system largely relies on workforce of local and municipal government authorities. If Centers for Disease Control and Prevention implements direct identification system it will protect human rights more effectively. There is an absence of the independent supervisory authority to prevent abuse or human rights violations.
- Unlike Germany's quarantine system to curb COVID 19 crisis, Korea's public health measures prone to infringe fundamental human rights. It seems like that the pandemic situation has pushed the lawmakers to enact public health legislations regardless of the proportionality principle. The recently passed public health regulation seems to have lost its original purpose of infection controlling by focusing on the restriction of citizens' behavior.
- The mass infection case in Itaewon suggested that personal information of contractors is a more serious matter to the sexual minority. Exposure of sexual identity could affect the daily life of them. They can be a target of exclusion or discrimination. Critics called for corrective action for personal privacy protection.
- While the guideline for personal data disclosure in contact tracing has been revised and recommended that personal identity should not be retraceable. The guideline, however, has no executive force, it has been not consistently implemented in local governments.
- As COVID 19 rages on, a lot of personal information are being collected and disclosed. Therefore, the management of sensitive data needs to be reinforced. It is a time that we have to rethink the value and perception of personal privacy. Human rights violation is a serious matter to social minorities. Thus, the flexible policy implementation methods and dual safeguards for minorities are also needed.

**[ Workshop #7 ] Request to the Korean Personal Information Protection Committee**

**Background** Globally, the emerging technologies like artificial intelligence and big data analytics have brought significant changes in the norms of personal information. While the shifts are underway, there is still considerable contention raised by stakeholders of data regulations. Recently Korean lawmakers have passed the '3 Data Acts' amid conflict and confrontation. From August 2020, the Personal Information Protection Committee (PIPC) has taken over its official duties with jurisdiction and comprehensive

authority to shape policies and practices on personal information protection. Previously the Ministry of the Interior and Safety and Korea Communications Commission has shared authority regarding personal data protection policy. It is now integrated into the PIPC. Accordingly, it is wondering what sort of priorities and principle to be set. Most of all, various stakeholders would like to hear expected role of the PIPC.

**Policy Questions**

- What should the PIPC's tasks with priority and what are the most urgent issues?
- Industries opinioned that PIPC should be renamed as Personal Information Committee laying less stress on personal information 'protection' itself. What is the role of the PIPC in this regard?
- What would be a relationship between the PIPC'a authority and government's data policy? How could the PIPC secure its independence ?
- What should be the operating principles that PIPC may keep in mind in light of Internet governance principle?
- Does the PIPC plan to participate in governance to establish global personal information framework ?

**Discussion**

- The most urgent task of the PIPC is to consistently adjust the legal provisions pertaining to personal information, which are still dispersed. The PIPC is also expected to play a pivotal role in coordinating various stakeholders' interests, and keep the general public informed about newly introduced concept of pseudonymized personal data.
- At first, adjustments in relation to the Financial Services Commission is needed since under Credit Information Protection Act, FSC is given authority regarding personal data.
- Industries are still questioning whether pseudonymized personal data can be properly utilized in statistics and scientific research purpose.
- It is necessary to reinforce the expertise of the PIPC members, expanding the capabilities of internal officers, and strengthening corporate responsibility of the industries.
- The independence of the PIPC is paramount. The body must be sufficiently protected personal data in the event of personal data leakage or damage and also it must play a role in providing adequate relief to the public with authority.
- As the PIPC'scope is closely related to consumers interests, so the voices of consumers should be reflected in the PIPC's practice.
- The PIPC should play a preemptive role in providing clear interpretation and guidelines for industries regarding deployment of new technologies that use personal information.
- Regarding the relationship between the PIPC and government's data policy, it is crucial that the PIPC's personnel affairs and budgeting must be independent from the central government. The PIPC should not be dominated by the industries or interests they are charged with regulating.
- Disclosing all gathered opinions of industries and users would be the best way to ensure its independence and expertise.
- The PIPC is an organization that should form social consensus on personal data usage and its protection. It would be ideal if the PIPC is inclined to gather more opinions and feedbacks from data subjects, whose voice is relatively small compared to industries.
- Industries contended that unquestioning acceptance of the European privacy protection framework would be not much desirable. Korea needs to focus on domestic settings and privacy perceptions relevant to personal information, and ponder on system suitable for the Korea's nature.

**[ Workshop #8 ] New Normal after COVID-19: Socially Underprivileged in the Untact**

**Culture**

**Background** As COVID-19 rages on non-face-to-face society became new normal. The untact (contactless) culture has taken root in Korea, it is widening the digital information gap. Untact culture is a trend of the new world, one that will continue even after COVID-19. It brought an issue of new information gap and exclusion. So we need to consider what we should to overcome digital exclusion. The definition of digital disparity has been recently redefined; its focus shifted from the level of physical accessibility to level of information use. According to the 2019 Digital Information Disparity Survey conducted by government, the digitally vulnerable groups suffered from the digital information gap — the disabled, low-income groups, the elderly, and farmers and fishermen— can literally have high physical accessibility to information. They, however, did not use it largely because of not knowing how to use it. Most of all, the level of technology literacy of them was quite low. As the untact culture has been pervasive, unmanned kiosk systems and digital devices unexpectedly has excluded a number of socially marginalized groups. The COVID 19 pandemic cast a task : how to deal with 'digital inclusion' for the groups suffered from information gap and digital divide. The workshop session looks into the stance of socially marginalized groups who are not much accustomed to newly adopted digital business services, brand new digital devices, and digital infrastructures with insufficient preliminary knowledge to survive in untouched culture.

**Policy Questions**

- How is Korean society changing due to the spread of untact culture and the acceleration of digital information?
- Are there any deficiency or additions to the 'digital inclusion policy' recently announced by the government?

**Discussion**

- Insufficient physical accessibility is not a problem anymore. As seen from recent survey that the digital information gap for the disabled is being resolved. In the case of people with disabilities, they once have recognized obstructive factors in the offline, but online world allowed the ways of interacting with others without being aware of their handicaps.
- Providing the disabled with assistive digital devices is necessary in an effort to increase their digital accessibility. Moreover, public digital services should contrive new ideas to increase accessibility from the design phase.
- Even users with severe disabilities are able to use social media services or administrative services with PC. The increase in technical capacity apparently brought positive effect on behalf of people with disabilities. As much as users' technical competence increases, the level of access to online services and information would be certainly improved.
- Basically, the settings that provide a lacked physical access to digital devices needs to be improved. In addition, in order to precisely evaluate the actual information gap that the disabled actually suffer, government will have to look into technical competence level of assistive devices.
- When it comes to digital inclusion, it is not desirable to force the government guidelines, to actors who are participating in socio-economic activities. As society becomes more digitalized, all actors are encouraged to collaborate together. What government should do is to elicit more positive effects with minimal regulation.
- After the outbreak of COVID-19 pandemic, a rapid transformation to non face-to-face is taking place. Therefore, the digital inclusion is increasingly regarded as important in light of fundamental human rights because digital exclusion or digital divide are affecting social and economic activities.
- Previously, the digital inclusion policies to improve the information gap had a limitation in that these only focused on basic Internet education for the vulnerable groups. But after COVID 19, the definition of digital inclusion has been expanded to all citizens. It aims at digital world without information disparity or digital exclusion.
- The digital inclusion policy is largely divided into four categories. i) education for

those who lack individual digital use capabilities, ii) ensuring accessibility that guarantees accessibility iii) technological R&D with supports for private companies, iv) establishing a public-private partnership that creates diverse digital social activities in which citizens can participate.

- Agreed to the minimization of government regulation, but it needs to be implemented in areas that need some regulation.

**[ Workshop #9 ] ICT-based Tracing in Response to COVID-19 : Striking a Balance Between Public health and Data Privacy**

**Background** As massive population have been infected with the coronavirus around the world, Digital-Contact-Tracing-Apps are being introduced in many countries. The tracing apps were developed to inform in case users have contacted with the confirmed patients through the bluetooth beacon technology. It is believed to contribute to preventing the spread of coronavirus since it suggests testing. The function of apps rely on API (Application Program Interface) of Google and Apple to track and notify contacts with patients. When a user installs the app on a mobile phone, it collects nearby smartphone records through Bluetooth. The installation of apps, however, is not mandatory. The Contact-Tracing-Apps got involved with data privacy concern. In Germany, 12 million people have downloaded the contact tracing apps but too few Germans use it. In France, only 1.5 million citizens have installed the StopCovid apps. With its utilization rate recorded less than 3%, it is regarded as a failure.

There are two ways to design the tracing app. The centralized model collects device data and stores it on a central server, whereas the de-centralized model exchanges necessary information only between users with anonymized data. The UK government announced a contact tracing app 'NHS COVID 19' insisting on a model that could aggregate anonymous data in a centralized manner. However, Apple declined to cooperate with UK government in designing a centralized tracing app. On the other hand, European countries prefer a privacy preserving de-centralized system. But even the installation rate of de-centralized model apps in European countries has not passed meaningful threshold.

In Korea, the public health authorities decided to deploy data-based technologies to response the emergency situation. Thus, data from GPS locations, credit card transaction records, transit pass records for public transportation, and CCTV footages are being used for epidemiological investigations. In addition, the Self-Quarantine Safety Protection App is a must for those who are subject to self-isolation during two weeks. It is using GPS technology to observe self-quarantine and unauthorized departure. ICT-based tracing itself does not mean abandonment of the value of privacy as far as the personal data are treated in pseudonymized form. Rather, it contributes to controlling the spread of coronavirus in the way of shaving time off to trace the infection route. Based on these evidence, Korea Centers for Disease Control and Prevention (KCDC) can detect lies and recommend testing if there were contacts patients with coronavirus. This workshop looked at the differences between the Contact-Tracing app in European countries, and pros/cos of ICT-based tracing system in Korea for epidemiological analysis in terms of data privacy.

**Policy Questions**

- What is the difference between Centralized model (France, UK, Australia, and Turkey) and, decentralized model (Canada, Germany, Switzerland, Italy) of contact tracing mobile app?
- What are the edges of ICT-based contact tracing in epidemiological investigation in case of South Korea?

- What is the ‘minimum’ range disclosure required for epidemiological investigations for public health purposes? How to ensure transparency and accountability in the collection and handling of personal data?
- What would be the negative aspects if the patient data are ‘excessively’ exposed? (social stigma, noncoopertive manner in investigations due to fear of exclusion)
- Why were local governments inconsistent in implementing ‘the guideline for personal data disclosure’ of coronavirus patients ?
- Are there any restrictions on how to use the collected data? What is the likelihood that the data could be used for purposes other than public health?
- Will personal data collected for public health purpose be deleted after a certain period of time? What if public health authority keeps these data for good?

**Discussion**

- Singapore, France, the UK, and Australia are the countries where the central government stores and manages personal data with the COVID 19 tracing app. Canada, Germany, Switzerland, Italy adopted decentralized tracing app. However, it is not effective because not much apps were downloaded due to the privacy concern. Meanwhile, in Coronavirus fight, Chinese government issued citizens a color code that contained information on individuals pose health risks and need to be quarantined. The QR-based health code system by Ali Pay and WeChat messenger are technology to police the country.
- European citizens are reluctant to use COVID-19 contact tracing apps that much. It is because of high sensitivity to privacy exposure, potential personal data leakage, distrust in data collection by government hands. The concern over privacy exposure is linked to a number of app downloads. So, contact tracing apps is not effective since across Europe, download rates of contact tracing apps have fallen short of enough numbers.
- The debate over how far it is appropriate to collect and retain personal data for public health purposes is taking place internationally. But epidemiological data collected for public health purposes in an emergency situation is inevitable.
- It is not desirable to disclose sensitive personal data that can easily re-identify the confirmed patients. When a certain patient’s identity is compromised, he/she becomes a target of criticism. Unnecessary social stigma effect can be caused by mere irrational speculation. This scenario is not helpful for public health. Patients feel fear, so they reject testing. It will increase the cost and time for tracking confirmed cases.
- In an emergency situation during COVID 19 pandemic, personal data collected centrally through ICT technology should be used for public health purposes. The gravity of life-saving measure far outweigh the disadvantages like data privacy concern. But there is a question as to whether the retention period is limited or will be deleted after a certain period of time.
- The practice of public health authorities and local governments must make a balance between personal privacy and public health. It is critical to balance the need for public health data to test, track, and quarantine with legitimate privacy concerns.
- In Korea, infectious disease prevention regulations take precedence over the Personal Information Protection Act, and the achievements of K-quarantine can be recognized globally when quarantine measures for public health and personal privacy are balanced.

**[Tutorial #1] The Global Landscape of AI Ethics Guidelines**

**Background** Over the past five years, global IT companies, research institutes, and public institutions have published the principles and guidelines for ethical artificial intelligence (AI). There is a growing consensus that AI should be ethical. But its elements, technical standards, and best practices are still unclear. As the discussion about global ethical AI standard is in full swing, it is necessary to review the core principles on ethical

AI.

**Content**

- Advanced economies are engaged in fierce competition in artificial intelligence (AI) in term of securing national competitiveness. There is a difference between the private sector represented by the IT industry and the public sector represented by the government in terms of potential dangers and AI ethics due to AI.
- The core ethical principles of AI are transparency, fairness, anonymity, explainability, and data privacy. *The Partnership on AI* that works with global IT companies in private sector such as Google, Facebook, Amazon, IBM, has already begun a review of AI ethics and governance in 2016.
- Meanwhile, the *Global Partnership on AI* launched in 2020. It is an AI policy council between countries, led by the governments of France and Canada, and the Secretariat is headquartered by the OECD. However, currently, policy making about AI governance seems till in the formative stage.
- Ethical AI itself requires a consensus process in which multi-stakeholders in phases of designing, and manufacturing. AI ethics of products and services can be set by technical standards by IEEE or ISO.
- Conflicting viewpoints are also emerging regarding ethical AI. For example , there is a growing awareness that AI can pose uncontrollable risks. But leading IT companies argue that risks are sufficiently controllable. The European Commission announced 'Ethics guidelines for trustworthy AI' emphasizing safety of AI. Meanwhile, Global South countries insist that AI should be shared in terms of "development" and "inclusion".
- There are diverging opinions : i) whether to define the category of AI as intelligent systems that act rationally ii) automated machines that think like humans. The different perception makes it difficult to form consensus on AI governance. Based on the level of technology currently implemented, AI is an 'acting rationally machine'.
- AI technology is getting more sophisticated, but there is no legal regulation that requires technical ethics and responsibility. The EC prefers policy to embody strict AI governance, but the White House in the U.S. implied that AI ethics should be left to self-regulation because it can hinder innovation.
- The private sector tends to emphasize the benefits of AI that consumers can enjoy, but AI ethics needs to be aligned with human values.
- The implementation of ethical AI is deeply related to technology standards setting and the design principles. The AI ethic principles should be based on broad consensus of machine learning architects, R & D researchers, manufacturers, and users. More internet users need to pay attention to AI ethics so that social costs and potential risks can be minimized and the majority can benefit from AI.

**[Tutorial #2] Now and The Future of Domain Name System (DNS)**

**Background** DNS has been around for over 30 years, but it still functions as a core infrastructure for domain-based Internet services. In the early days of internet, there were only a few national top-level domains (. kr) and some general top-level domains (. com, . org). But as of 2020, more than 1,500 top-level domains are available. And the vast DNS networks have been working based on the DNS root zone. DNS has not changed the basic purpose of converting IP addresses into domain names, but internally it has undergone remarkable development. The 512-byte size restriction no longer exists, and the root DNS has been extended to more than 1,000 nodes through Anycast technology. In addition, DNSSEC technology was introduced to prevent DNS forgery, and new technologies – DoT, DoH – were being developed, as the the value of data privacy protection and security were recognized. Although DNS has been a gateway service to the Internet for a long time and in the future, its importance is not well known to most internet users. This tutorial aims to deliver various topics related to DNS to the general public in an easy-to-understand manner, from basic concepts such as the role and basic operation of DNS, the relationship between root DNS-kr DNS-user DNS, to the latest topics such as DNSSEC, DoT, and DoH.

**Content**

- DNS was first developed in 1983 and is still in use as a methodology that maps IP addresses that are difficult to memorize and complex on the network to domain names.
- How DNS works and Domain query procedure?
- DNS features-Distributed database, tree-structured domain name system
- DNS record-Define the type of information that DNS responds
- Domain name configuration: Label, unique name, FQDN (Fully Qualified Domain Name)
- DNS management: Classification of name servers-Authorization DNS and cache DNS, master name server and slave name server
- DNS server redundancy/multiplex configuration
- Domain delegation settings, and Internet ecosystem and DNS ecosystem
- National domain registration information and national DNS reflection procedure
- Major stakeholders of the DNS ecosystem (ICANN, IANA, RSO, TLD registry, etc.)
- Example of DNS governance operation (DNS Flag Day)
- Background of DNSSEC (Domain Name System Security Extensions)
- DNSSEC operation principle, trust chain, trust anchor
- DNS and Privacy-DoT/DoH Overview
- Universal DNS-DNS as a global distributed DB

**[ Open Consultation #1] WHOIS Domain Privacy Policy under the New Personal Privacy Protection Law of Korea**

**Background** The Internet Address Resources subcommittee is a part of the Korea Internet Governance Alliance (KIGA) where various stakeholders openly discuss and gather opinions on Internet domain name policies. Open consultations are held to hear a wide variety of opinions. Anyone can participate and hear how the Internet Address Resources subcommittee has been working on what kind of issues are pending.

**Content**

- WHOIS Policy: The WHOIS database, which discloses Internet domain name registrants and related information, is changing globally with the entry into force of the European Personal Information Protection Act (GDPR). In line with this, we need to discuss how to change the domestic WHOIS information disclosure policy. For example, there has been a contention over whether to disclose the name of the corporate registrant, the name of the person in charge, and phone number of the technical manager.
- Discussions about .or.kr domain policy: .or.kr domain names are supposed to meet the non-profit registration criteria. But in practice, companies, organizations, and individuals also can register .or.kr domain names. Therefore, it came to be debated on whether to keep the registration criteria should be applied to companies, organizations, and individuals for commercial purposes. Otherwise, should we keep the public resource nature of .or.kr domain as it had been? It would be one of domain name policy decisions in the near future.
- Discussion about a draft of amendment of Internet Address Resource Act, and domain name registration rules, etc.