DIGITAL ASIA HUB

ArtEZ

KELLY KIM 켈리 킴 케리 킴 凱丽・金

DEV デヴ・ルイス 데브 루이스 LEWIS 戴逸司

スミサクリシュナプラサド 스미타 크리슈나 프라사드 SMITHA KRISHNA PRASAD 思米沙・克里希那・普拉萨德 सिमिता कृष्णा प्रसाद

PLATFORM FUTURES

PLATFORM FUTURES

Small Books for Big Platforms

Book 2.

Data Opportunities and Challenges

Kelly Kim Dev Lewis Smitha Krishna Prasad

Gayatri Khandhadai Nishant Shah

Table of Contents

Introduction

Small Books for Big Platforms — Book II: Data Opportunities and Challenges

Editor

Nishant Shah

The ‘Small Books for Big Platforms’ series, part of the Digital Asia Hub’s programme on Platform Futures, is a comparative cross-area study that explores the opportunities and challenges of data ecosystems and platform ecologies in the Asia-Pacific region. It invites scholars studying the policies, regulations, implementation, digital cultures, and usage of emerging and existing platform structures in the region to provide a critical insight into the multiplicity, potentials, and ramifications of platform societies.

The ‘platform’ in these books is not a monolith: it encompasses a multiplicity of practices, histories and cultures in different parts of the world. Both books revolve around the idea of frictions, particularly when it comes to understanding the emergence, affordances, and governance of platforms.

The ‘small books’ are meant to be sharp, critical, located studies that help map the field as well as develop an inventory of questions that emerge from the localisation of platforms and the regional geo-political landscape within which they operate. The books simultaneously want to foreground the specificity and difference in emerging platform societies, thus demanding for granularised and located understanding of platformisation, as well as the larger shared concerns and connections that help strengthen the continued conversations around competition, innovation, safety, security, privacy, transparency, and distribution

of data- and algorithm- driven practices on digital platforms.

Meanwhile, the series is also meant to be provocations that help understand the emerging policy issues, the discourse in different regions, and the opportunities and threats of platform futures in the Asia Pacific region. It is particularly keen on provoking discussions around the ‘frictions’ of platforms, which do not necessarily follow the discourse of a largely North-West centred theoretical and cultural orientation. We use ‘frictions’ as a space of provocation because it doesn’t offer easy polarisations or binaries, but instead looks at the process through which the platformed societies operate and work, and the spaces where they ‘don’t quite sit well’. ‘Frictions’ could be enablers or barriers, causes or symptoms, or points of tension that highlight pre-existing contestations or histories. Instead of platforms as blackboxes, we approach them as ‘spaces in the making’, and are interested in mapping the different actors, stakeholders, communities, and users who make the platforms and create conditions for their emergence and adoption.

The first two ‘small books’ are a starting point of this series. Each ‘small book’ has a defined theme that focuses on Mobile Ecosystems and Data Opportunities and Challenges. Given the fluidity of these focus areas, the tensions and the local urgencies of these emerging fields, it was necessary for us to conceive of these ‘small books’ as collaborative, community- driven projects which centre the scholarship of renowned scholars

and practitioners rooted in multi-discplinary and multi-sectoral engagements. It is important for us to emphasise that while the scholarship in this book is developed by the authors giving us meaningful and nuanced contributions, it is bolstered by a larger community of peer-reviewers, who have engaged with this work and added to it through a distributed open-review process, participation in workshops, and conversations and dialogues that go beyond the scope of these books. We would like to express

Chinmayi Arun	Resident Fellow, Information Society Project, Yale Law School
Nighat Dad	Executive Director, Digital Rights Foundation
Bishakha Datta	Executive Director, Point of View, India
Kingwa Fu	Associate Professor at the Journalism and Media Studies Centre of The University of Hong Kong
Helani Galpaya	CEO, LIRNEasia
Yong Lim	Co-Director, AI Policy Initiative, Seoul National University
Siddharth Narrain	Phd Candidate, School of Global and Public Law, Faculty of Law and Justice, University of New South Wales
Julian Thomas	Director of the ARC Centre of Excellence for Automated Decision-Making and Society, and a Distinguished Professor in the School of Media and Communication, RMIT University.

In this ‘small book’, around the theme ‘Data Opportunities and Challenges’, Smitha Krishna Prasad, Kelly Kim, and Dev Lewis contributes key written inputs that pay particular attention to Covid-19 and public health platforms in India, data opportunities and challenges in South Korea, and Taiwan model for civic-tech platforms in the Covid-19 pandemic. Each contribution provides a synthesis of the state of discourse in the field, landmark policies, judgements, regulations, practices, and cases that shape this discourse, a detailed analysis of the challenges and opportunities presented, and further considerations and recommendations on interventions that are needed to build more equitable, resilient, and inclusive futures of platformisation. What’s more, one synthesis piece, developed by Gayatri Khandhadai, is included and provides a bird’s eye view of the emerging knowledge within this theme. With its multi-area focus and Inter-Asia-Pacific framework, we hope that these small books become a vehicle of asking big questions about platforms that our futures are being hosted on.

Synthesis

Understanding Data Opportunities and Challenges through Experiences

Gayatri Khandhadai

The chapters on India, South Korea and Taiwan come at a time when there is great division among stakeholders on their positions on data and its governance. Rapid data utilisation has been promoted as the only way forward for development and progress across the region. The COVID-19 pandemic has enabled many states to leverage public and personal data towards developing solutions or responses. This small book helps us look at data governance from regulatory, participatory, and security narratives.

The three chapters talk of vastly varying contexts. While the chapter on South Korea presents an objective outlook on the regulatory framework on data governance, the chapters on Taiwan and India discuss the use of data for democratic governance and to cope with the deadly COVID-19 pandemic. The experiences of Taiwan and India are dissimilar in many ways, as they present fundamentally opposing styles of governance and partnership. Meanwhile, access to the internet and digitalisation are not evenly experienced across these three states. South Korea has the largest internet penetration in the region, Taiwan is seen as a pioneer in public participation and civic tech, whereas in India there is a significant digital divide or lack of meaningful access to the internet.

"Recent Debates on Data Utilisation and Protection: 3 Data Laws and Lee Luda" authored by **Kelly Kim** of Open Net Korea, maps

the history of information and communications technologies (ICTs) and platform development in South Korea alongside the evolution of data governance and protection systems or frameworks. The paper explores tensions between data utilisation and data protection in the laws that govern them. The Personal Information Protection Act, the Act on the Promotion of the Use of the Information Network and Information Protection, and the Credit Information Use and Protection Act are discussed to provide an overview of protections and provisions that enable data utilisation. Instances of datasets of communication, video game, and credit card platforms being hacked, resulting in the compromise of the personal data of millions of individuals, are presented as one of the bases of the demand for greater protection. Kim has explored the lack of sufficient protections in pseudonymisation through theoretical and experiential perspectives. Lee Luda, an AI chatbot created by ScatterLab, is presented as an interesting case of how pseudonymisation was defeated, as it was able to identify personal information and engage in hate or discriminatory speech. This indicates data breach, illegal use of data and the lack of safeguards. The paper thus illustrates the tensions between different stakeholders in a context where there is an evident political push in the name of the 'fourth industrial revolution' favouring data utilisation over data protection, resulting in discontent among users and civil society.

"Taiwan's COVID Response" by **Dev Lewis**, provides a fresh

take on the possibilities of using data for public good, by enabling public participation. This paper draws on many examples of public partnership, open source technical solutions and consultative processes for emerging governance and health-related challenges ultimately resulting in greater trust and community ownership of initiatives. Lewis outlines efforts taken for rationing and distribution of masks during the COVID-19 pandemic with the use of National Health Insurance (NHI) cards and collaboration with multiple developers who were able to build on the application for decentralised access through various interfaces or technologies. vTaiwan and Join.gov are examples of how the state enables public participation in policy and executive decision making. These efforts have made way for greater transparency, citizen participation and communication. The use of data, AI and machine learning to gauge public sentiment in relation to policies is illustrated with the example of how Uber was regulated in Taiwan. Lewis points to this example as a process for consensus building among stakeholders which relies on data and transparency, including through a live streaming of deliberations. Taiwan's approach is directed towards decentralised, collaborative and people-centred data use, using a bottom-up process aimed essentially at participatory decision making and trust building.

The final chapter, "Covid-19 and Public Health Platforms in India" authored by **Smitha Krishna Prasad**, paints a different

picture of realities in a context where there is a deep digital divide causing the exclusion of millions. Against the backdrop of unimaginable loss and suffering caused by the second wave of the COVID-19 pandemic, Prasad presents the different technological solutions deployed by the state with specific emphasis on the Arogya Setu contact tracing application. The paper discusses the evolution of this contact tracing application and concerns around the lack of transparency and guarantees on data protection impacting millions of Indians. Existing regulatory frameworks and programmes that govern public health services are showcased with the observation that they lack information on how privacy and security concerns should be handled. Similar worries are raised in relation to India's vaccine registration application, COWIN. The lack of a comprehensive law on data protection is cited as a significant hurdle and the author goes on to discuss the merits and problems with the Personal Data Protection Bill, 2019, which is currently under deliberation. These form the basis of questions around the state's plans to digitise health data and provide Digital Health IDs. Through these examples, the author asks if technology is the only or right way to deliver solutions, and cautions against pushing out hastily built solutions which may end up causing exclusion and other long-term harm.

The papers on India and South Korea point to the clawback clauses embedded in data protection regulations, especial-

ly those that negate prohibitions in the name of research for commercial or development purposes. They have made a call for predictable and transparent regulation and guidelines with oversight and accountability. Revising approaches to informed consent are also presented as a crucial need. The Taiwan experience inspires confidence in the good that can come out of principled partnerships and collaborations. The book will help us revisit our approach to data governance and question whether the regulations we are subjected to have been developed in a people-centric manner and are governed with a human rights-based approach that responds to the demands and technological evolution of our times.

Kelly Kim
Open Net Association

Recent Debates on Data Utilisation and Protection: 3 Data Laws and Lee Luda

Introduction

Korea's Internet and Platform History

Korea, with the world's highest smartphone penetration rate (KBS World 2019) will be the next country, after the US — except for China with the Great Firewall — where local platforms thrive. Naver against Google, KakaoTalk against WhatsApp, and Coupang against Amazon are boasting overwhelming market shares. Although Korea is now undoubtedly an Internet powerhouse, Korea's information and communication infrastructure was poor until the 1980s. However, with the establishment

of a System Development Network (SDN) by the Korea Institute of Electronics Technology (KIET, presently ETRI [Electronics and Telecommunications Research Institute]) and Seoul National University on May 15, 1982, Korea became the second in the world after the US, and the first in Asia, to develop TCP/IP-based Internet (Chon et al. 2005). Dr. Kilnam Chon, who led the development of SDN, is called the “father of the Korean Internet” and was inducted into the ISOC Internet Hall of Fame in 2012.

In 1994, Korea Telecom (KT) launched a commercial Internet service, “KORNET”, and the number of Internet users surpassed one million in 1997. In 1999, just a year after Thrunet launched the first broadband Internet service in 1998, the number reached ten million. In 2001, the OECD announced that Korea ranked first in the world in terms of broadband penetration rate (Moon 2020, 12). Korea launched the world’s first commercial CDMA mobile phone service in 1996 and achieved ten million mobile phone subscribers in 1998. Small territory and high population density played a part in such remarkable development, but above all, the government’s aggressive implementation of informatisation policies and the voluntary participation of the private sector centered on schools and research institutes played a major role. The history of Korean platforms can be traced to the mid-1990s when a number of venture companies came into being as a result of this infrastructure. In 1995, JoongAng

Ilbo launched the first Internet newspaper service in Asia. In 1996, Interpark launched the Internet shopping mall service, and Nexon released the world's first graphic MUD (Multi-User Dungeon) game "The Kingdom of the Winds."[1] In 1997, Daum Communications launched the Hanmail service, and Samsung SDS' first in-house venture project Naver launched a Korean search engine. In 1998, NCSoft released MMORPG (Massively Multiplayer Online Role-Playing Game) "Lineage".

With the advent of commercial broadband Internet services, Korean platforms exploded in the late 1990s. In 1999, Korea's first web portal Daum was launched, the first internet banking service began, and the world's first web-based chat service Sayclub was launched. Moreover, the world's first VoIP (Voice over Internet Protocol) Dialpad, developed with Korean technology, started offering their service for free in the US. The search engine Empas was launched and competed with Naver. In 2000, a social media service Cyworld was launched — four years earlier than Facebook. In 2004, the number of internet users in Korea exceeded thirty million, and in 2005, the Korean online game market exceeded one trillion won (Ahn and Kang 2014, 200). AfreecaTV, a live-streaming platform, was launched in Korea in 2005 — the same year YouTube was established. A mobile messenger KakaoTalk was launched in 2010, and has contin-

1 The Kingdom of the Winds was listed in the Guinness Book of Records in September 2010 as the world's first commercially available graphic MMORPG, and in 2011, it was again listed as the longest serviced graphic MMORPG.

ued to be the number one messaging app since its launch (Oh, Hong, and Lee 2020).[2]

Data Opportunities and Challenges Faced by Korean Platforms

The data opportunities and challenges faced by Korean platforms can be rephrased as the tension between data utilisation and data protection. Data is often called "the new oil" in the age of the Fourth Industrial Revolution. Data is essential for the development of products and services based on cutting-edge ICTs such as artificial intelligence (AI), big data, and cloud computing. Data utilisation is at the core of the Fourth Industrial Revolution policies and the Digital New Deal Initiative of President Moon Jae-in, who took office in 2017.

On the other hand, a combination of the resident registration system assigning every citizen a unique identification number from birth, policies mandating collection of personal information such as the mobile phone registration system and the Internet real-name system, and a culture insensitive to privacy infringement has resulted in numerous personal data breaches, leading to ever increasing calls for a stronger data protection regime. In response, the Personal Information Protection Act was enacted and the Personal Information Protection Commission (PIPC) was established in 2011, long before the GDPR was enacted in the EU. Korea now has one of the strictest data protection regimes in the world, albeit nominally. Accordingly, there has been

2 KakaoTalk is used by 87% of the Korean population (about 45 million people) in 2020, and it had 99.2% of the messenger app share in 2018.

tension between the industries wanting to use data freely and users and civil society worrying about privacy infringement, with the government trying to coordinate these different needs. This conflict was particularly highlighted in the amendment process of “3 Data Laws” in 2020, which focused more on data utilisation than protection.

I will briefly introduce Korea’s data protection laws and policies, key stakeholders and their positions, and look at the AI chatbot Lee-Luda case, which epitomises the main issues of the recent conflict between data utilisation and protection in Korea.

3 Data Laws and Policies on Big Data

Amendment of 3 Data Laws in 2020

“3 Data Laws” amended in 2020 are the Personal Information Protection Act (PIPA), the Act on the Promotion of the Use of the Information Network and Information Protection, etc. (ICNA), and the Credit Information Use and Protection Act (CIA). 3 Data Laws’ amendments focusing on the utilisation of data have been controversial since their inception. Because data protection and utilisation are often inversely related, there were concerns that only data use would be promoted while data protection being neglected. Nevertheless, the amendments were passed by the National Assembly on January 9, 2020, after many twists and turns, and 3 Data Laws became effective on August 5, 2020.

The most important of the 3 Data Laws is the PIPA. The PIPA

was enacted in 2011 and replaced the Act on the Protection of Personal Information of Public Institutions, which was enacted in 1994.[3] Prior to the enactment of the PIPA, personal information protection in the private sector was in the legal blind spot. Along with the advent of the digital age, the importance of data protection emerged, and the PIPA was born. The CIA, which was enacted in 1995, introduced concepts of "credit information" and "personal credit information" and required financial firms processing credit information to obtain permission from the Financial Services Commission. The ICNA is the oldest of the 3 Data Laws and is the successor of the Act on Expansion of Dissemination and Promotion of Utilization of Information Systems enacted in 1986. The provisions on personal information protection, however, were included only in 1999 when it was revised to become the ICNA.

Ironically, the history of Korea's data protection is a history of data breaches. In January 2008, the personal information of eighteen million users of Internet shopping mall, Auction, was stolen. In 2011 — the year the PIPA was enacted — the database of SK Communications, which operated web portal Nate and social media Cyworld, was hacked, and the personal information of thirty-five million people was leaked. In the same year,

---

3 The reason why the data protection regime was first introduced in the public sector in Korea is deeply related to the establishment of administrative computer networks, which began in the late 80s. While the networks and the computerization of administration enabled the full informatisation of administration, there were concerns about various side effects, such as privacy violations caused by unauthorized use or leakage of personal information.

the personal information of thirteen million users of video game publisher Nexon was compromised. In 2014, a series of massive scale data breach incidents occurred. The personal information of subscribers of three credit card companies — KB Kookmin, NH Nonghyup, and Lotte Card — was compromised by security personnel. Personal information leaked from the three card companies amounted to 104 million cases — twice the Korean population. Within three months of this data breach, the hacking of KT's website leaked the personal information of twelve million people (Lee 2020).

As the call for more robust data protection increased due to the series of data breaches, the PIPA was revised in 2016. The reform introduced punitive damages and criminal punishment, significantly strengthening the regulation of data processors. However, four years later, the atmosphere changed with the rise of voices demanding the use of data. The government and the National Assembly, paying attention to the trend of the Fourth Industrial Revolution based on data-driven technologies around the world, pushed for the amendment of 3 Data Laws, which focused on data utilisation.

Introduction of Pseudonymised Information

The most important amendment of 3 Data Laws concerns "pseudonymised information." The revised PIPA introduced the concept of pseudonymised information with reference to the GDPR.

Pseudonymised information is personal information that has undergone pseudonymisation and "thereby becomes impossible to identify a particular person without the use or combination of additional information for restoring the information to its original state" (Article 2 subparagraph 1 (c)), and "pseudonymization" is defined as "the processing of personal information by deleting in part, or replacing in whole or in part, such information so that the information cannot identify a particular person without additional information" (Article 2, subparagraph 1-2). On the other hand, the PIPA stipulates "special cases for the processing of pseudonymized information," allowing a personal information controller to process pseudonymised information without the consent of a data subject for statistical purposes, scientific research purposes, and archiving purposes in the public interest (Article 28-2). In particular, "scientific research" is defined as "research that applies scientific methods such as development and demonstration of technologies, fundamental research, applied research and privately-funded research" (PIPC n.d.). This opened the way for the use of personal information to develop new technologies, products, and services based on data. As such, the main purpose of the 3 Data Laws reform was to enable the utilisation of pseudonymised information without the consent of a data subject.

In September 2020, only a month after 3 Data Laws came into force, the PIPC published the "Guideline for Processing of Pseu-

donymized Information." The Guideline is largely divided into three chapters: "Pseudonymization," on the procedure of pseudonymisation for a personal information controller to use personal information; "Combination of pseudonymized information," on the combination and release of pseudonymised information held by different personal information controllers; and "Safe management of pseudonymized information," on managerial, technical, and physical safety measures for pseudonymised information.

The Fourth Industrial Revolution and Big Data Policies

President Moon Jae-in had emphasised the Fourth Industrial Revolution even before his assumption of office in 2017 (Park 2017) and proposed "the Fourth Industrial Revolution Leading the Development of Science and Technology" as a key economic strategy for 100 Policy Tasks (CHEONGWADAE n.d.).

According to the strategy, the Ministry of Science and ICT (MSIT) was entrusted with the responsibility of building infrastructure and improving regulations for the Fourth Industrial Revolution, and the Presidential Committee on the Fourth Industrial Revolution (PCFIR) was established. The strategy specified the "facilitation of data opening and distribution" as its main contents.

The Fourth Industrial Revolution is a hyper connectivity-based intelligent technology revolution, triggered by the development of AI, big data, and other digital technologies, expected to give rise to innovative transformations in not only industries but also

the national system, society, and people's everyday lives (The Government of the Republic of Korea 2017, 12). It is heralding innovations at an unprecedented, exponential scale on all fronts through the convergence of diverse areas and industries based on intelligent information technologies such as DNA (Data-Network-AI). It is also an upgrade from "informatization" to "intellectualization" based on AI. Therefore, the success of the revolution depends on the level of AI, and AI in turn greatly depends on big data. After all, big data is both the output and driving force of the revolution (Jeong 2018, 2). The PCFIR was established to review and coordinate policies related to the Fourth Industrial Revolution and promote advances. Its role expanded to become a national data policy control tower in 2020 and it strives to bolster the data-based digital economy. It is against this backdrop that 3 Data Laws were revised by the current government.

In 2016, before the 3 Data Laws reform, the government published the "Guideline for De-identification[4] of Personal Information" to facilitate the use of big data. Until then, the industry had complained that the standards for de-identification were not clear, making it difficult to use big data. In addition, academia and the media consistently pointed out the need for guidelines to respond to the demand for data utilisation, resulting from

---

4 "De-identification" means the process of removing personally identifiable information from certain data, and the term is often used in the same sense as "anonymization." The term "de-identification" is commonly used in countries such as the US, and the term "anonymization" or "anonymous processing" used in the EU and Japan, but the two terms are generally interchangeable (Shim 2017, 2).

the development of new technologies such as big data and the convergence industry. Accordingly, the government developed the Guideline to promote industrial development by eliminating uncertainties while preventing data breaches (MOIS 2016). The Guideline for De-identification stipulates standards for de-identification and the scope of use, and allows companies to combine customer information with information held by other companies through specialised agencies such as the Korea Internet & Security Agency (KISA). Twenty domestic companies, including three major telecommunications companies, have combined and utilised 340 million sets of personal information through these specialised agencies. However, in November 2017, civil society organisations including the People's Solidarity for Participatory Democracy (PSPD) reported four agencies and twenty companies to the Prosecutors' Office, for the violation of data protection laws (PSPD 2017). The case was dismissed (Kim 2019), but the companies became defensive and the Guideline is now a dead letter.

Key Stakeholders Involved in 3 Data Laws

Before the amendment of 3 Data Laws, it was difficult to consistently respond to problems related to data protection, because the authorities in charge of each law were different and there were many similar and overlapping provisions. The PIPA governing the public and private sectors was under the jurisdiction of the Ministry of Interior and Security (MOIS) and the

PIPC, the CIA governing the financial sector was under the jurisdiction of the Financial Services Commission (FSC), and the ICNA governing IT industries and platforms was under the jurisdiction of the Korea Communications Commission (KCC). The amendment transferred the chapter on data protection in the ICNA to the PIPA and reorganised overlapping data protection provisions in the CIA. In addition, the PIPC was elevated to the status of a ministry.

As I mentioned earlier, the current administration's policy stance clearly favored data utilisation over data protection. President Moon Jae-in has been emphasising the importance of the Fourth Industrial Revolution, and the PCFIR was the initial driving force behind the 3 Data Law amendments (PCFIR 2020). On August 31, 2018, President Moon declared a "Transition to the Data Economy," and in line with this, the government announced a plan to foster data industries and innovate data regulations to promote the data economy (MCST 2020). In July 2020, President Moon announced the Korean New Deal Initiative, which has the Digital New Deal as one of its two main pillars (CHEONGWADAE 2020). "Digital Dam," the core of the Digital New Deal policy, aims to "accelerate the data economy by strengthening the basis for data collection, processing, transaction, and utilization and spread 5G and AI convergence in all industries through the nationwide 5G network" (CHEONGWADAE n.d.). The IT industry and platforms have continuously demanded

that data protection regulations be relaxed so that data can be used more freely. In 2019, the Korea Internet Corporations Association (K-Internet), Korea Startup Forum, Korea Association of Game Industry, and other industry stakeholders urged the legislation of 3 Data Laws, stressing that technology-neutral regulation reforms embracing “data protection” and “safe data utilization” are crucial in order for Korean internet companies to lead the era of the Fourth Industrial Revolution (K-Internet 2019). Civil society, which has consistently called for stronger data protection, had opposed the 3 Data Laws amendments, calling them the “Data Theft Laws,” and is now requesting another reform (PSPD 2020). Regarding pseudonymised data, Open Net has pointed out that the “scientific research” purpose allowing non-consensual use of pseudonymised data requires publication of the research like the GDPR implies, and that Article 28-7 of the PIPA depriving data subjects’ access and other rights to pseudonymised data should be amended (Open Net 2021). Civil society also severely criticised the Digital New Deal policy, saying that the government’s approach to data was lopsided and the policy meant selling the people’s privacy for economic growth (Jinbonet 2020).

AI and 3 Data Laws in light of Lee Luda

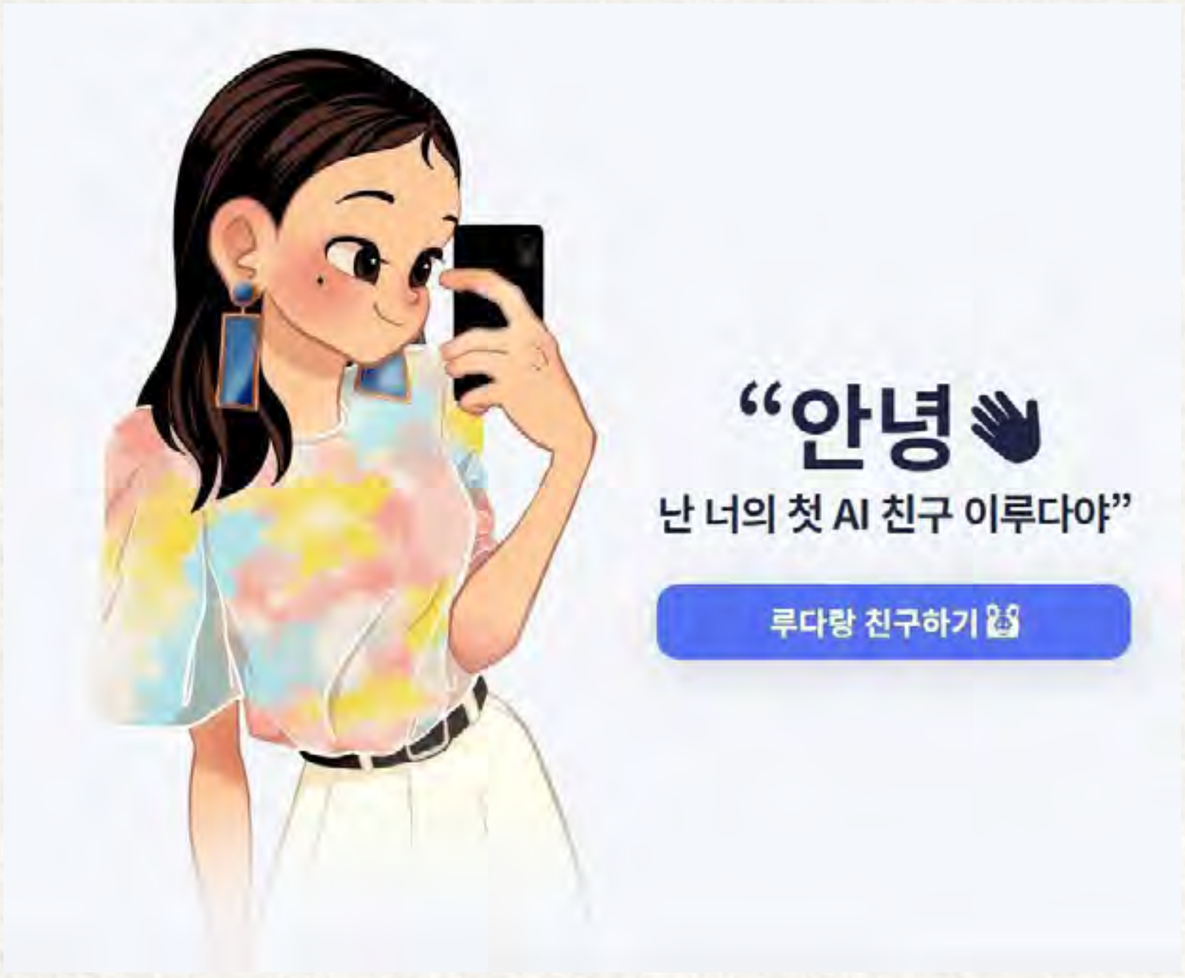
Overview of the Case

The AI industry will benefit most from the 3 Data Law amend-

ments. AI is a key industry in the fourth industrial revolution and data economy, with not just the private sector but the government also making huge investments. In this context, it is worth examining the AI chatbot “Lee Luda” case as it encompasses all recent AI issues, from AI ethics to data protection in Korea.

Lee Luda was an AI chatbot service developed by ScatterLab, Inc., launched on December 23, 2020. She had a virtual profile of a 20-year-old female college student with the catchphrase “Hi, I’m your first AI friend Lee Luda.” People could add her on Facebook messenger. The MZ generation — Millennials and Gen Z — were enthusiastic because Lee Luda felt like a natural person as she was trained in real conversations. She became very popular and attracted more than 400,000 subscribers in two weeks. However, like Microsoft’s Tay, Lee Luda’s hate speech and discriminatory remarks against minorities became an issue. Then the controversy about a data breach arose, as some conversations revealed people’s names, addresses, and even bank account numbers. Some pointed out that the training data was illegally collected and used (PSPD 2021). Eventually, public sentiment rapidly deteriorated, and ScatterLab had to pull down Lee Luda merely twenty days after its launch. The PIPC, together with KISA, started an investigation in January 2021, and on April 28, fined ScatterLab for a total of 103.3 million won for the violation of the PIPA (Choi 2021). Aside from this, in March, 245 users filed a class-action lawsuit against

ScatterLab for privacy infringement (Lee 2021).



AI chatbot Lee Luda. Lee Luda's homepage image.

The issues are largely divided into two. The first is the ethics and bias of AI, and the second is data protection. The first issue is less relevant to the subject of this article, so I will examine the data protection issue in detail below.

Data Protection Issues of Lee Luda

Consent to purposes of data collection. According to the findings of the PIPC, ScatterLab used KakaoTalk chat logs collected from its other services, "TEXTAT" and "Science of Love," in the development and operation of Lee Luda. Both are services that analyse KakaoTalk conversations and provide dating counseling. ScatterLab used about 9.4 billion KakaoTalk sentences from about 600,000 users and built a response DB with 100 million sentences for the operation of Lee Luda. ScatterLab argued

that the use of data was legitimate, as users gave consent to the collection and processing of chat logs for the "development of new services" as indicated in its privacy policy. However, the PIPC found that ScatterLab did not receive legitimate consent and used the data for a purpose different from the purpose of collection and cited the following reasons:

1. it is hard to determine that the users gave consent to "development of new services" just by including that phrase in TEXTAT and Science of Love's privacy policies and interpreting logging-in as giving consent;
2. it is also hard to expect users to know that "development of new services" includes using KakaoTalk chat logs for the development and operation of Lee Luda; and
3. users may suffer unpredictable damage such as restrictions on their privacy.

Pseudonymisation or De-identification of Personal Information.

As personal information such as names and addresses were exposed in Lee Luda's chats, it became controversial whether pseudonymisation of the training data was properly performed. ScatterLab said that the data had undergone a de-identification process and was made up of separate and independent sentences, making it impossible to identify individuals. However, some information, such as names, were left untouched because perfectly de-identifying informal daily conversation, unstructured data, is difficult. This meant that Lee Luda repeated

these imperfect sentences when composing its responses to users. Civil society criticised 3 Data Laws because it allowed companies like ScatterLab to freely use personal information for service development without receiving consent from the data subject, as long as they pseudonymised personal data (PSPD 2021). More specifically, the GDPR allows non-consensual use for the "scientific research" purpose in the public interest, while 3 Data Laws allow commercial use of pseudonymised data without consent (Open Net 2021). In addition, some pointed out that the PIPC's "Guideline for Processing of Pseudonymized Information" is insufficient to be used as a standard for handling unstructured data (Shin and Jeong 2021, 3). Unfortunately, the PIPC did not investigate whether the training data was properly pseudonymised or whether it constituted non-consensual use of pseudonymised data as "scientific research." It only found that ScatterLab violated Article 28-2 (2) of the PIPA, which prohibits providing pseudonymised data including identifiable information to a third party,[5] because ScatterLab uploaded 1,431 KakaoTalk sentences on GitHub, which included identifiable information such as names.

Recommendations

The main reason why ScatterLab was fined was because the consent given by users was inappropriate. Nowadays, con-

5 Article 28-2 (Processing of Pseudonymous Data) (2) A personal information controller shall not include information that may be used to identify a certain individual when providing pseudonymised information to a third party according to paragraph (1).

sent-requirement has become a mere formality, and such a consent system can be abused as a means to justify data collection and use, rather than guaranteeing the data subject's rights. It is necessary to simplify and substantiate the consent system to increase its effectiveness and strengthen ex post facto control. Since AI can automatically collect and process personal information without human intervention, by using technologies such as web crawling and the IoT (Internet of Things), it is essential to properly combine the ex-ante consent system and the ex-post control system. Moreover, it needs to clearly define the scope of "scientific research" which allows the non-consensual use of data through pseudonymisation. Secondly, it is necessary to improve the Guideline and promote research on pseudonymisation technology and methodology when it comes to unstructured data. In order to do that, the cumbersome procedural requirements for pseudonymisation must be streamlined. Pseudonymisation is not only good for research and development but also for the protection of privacy. As GDPR recommends, it acts as both a security measure and privacy measure by design. Thirdly, the competitiveness of AI lies in securing training data. However, many SMEs and start-ups struggle to secure data and are incapable of pseudonymisation. Therefore, the government's investment and support are crucial.

Conclusion

Korean platforms have grown remarkably in the last few

decades, thanks to the world's best ICT infrastructure.

The biggest friction currently faced by the platforms is happening in the area of data protection. Conflicts have continued between the industries demanding unrestricted data use, users and civil society concerned about privacy, and the state trying to coordinate different needs. The stakeholders sharply confronted each other in the amendment process of 3 Data Laws. Lee Luda provided a concrete, real-life example of this conflict that questioned everyone about the way forward. Data protection and utilisation are not antitheses to each other. All stakeholders should continue to make efforts to improve the laws and systems so that safe data utilisation without compromising privacy becomes possible.

References

Ahn, Jungbae and Kang, Kyungran. 2014. 한국 인터넷의 역사 , ㈜블로터앤미디어.

CHEONGWADAE. 2020. “Keynote Address by President Moon Jae-in at Presentation of Korean New Deal Initiative.” Cheongwadae, July 14, 2020. https://english1.president.go.kr/Briefingspeeches/Speeches/852.

———. n.d. “국정과제.” https://www1.president.go.kr/government-projects#page2 (Accessed July 30, 2021).

———.n.d. “한국판 뉴딜.” https://www1.president.go.kr/KNewDeal (Accessed July 30, 2021).

Choi, Hongsuk. 2021. “개인정보위, ‘이루다’ 개발사 ㈜스캐터랩에 과징금·과태료 등 제재 처분.” PIPC, April 28, 2021. https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298.

Chon, Kilnam et al. 2005. “A Brief History of the Internet in Korea.”한국 인터넷 역사 프로젝트. August 29, 2005. https://sites.google.com/site/koreainternethistory/publication/brief-history-korea-eng-ver.

Jeong, Joonhwa. 2018. “4차 산업혁명 시대의 빅데이터 정책과제.” National Assembly Research Service (NARS), July 4, 2018.

Jinbonet. 2020. “디지털뉴딜, ‘국민사생활’ 팔아 경제성장하겠다는 것.” 진보네트워크센터. Jinbonet, July 21, 2020. https://act.jinbo.net/wp/43213/

K-Internet. “인기협 등 5개 단체, 국회에 개인정보보호법 개정안의 조속 처리 촉구.” K-Internet, September 26, 2019. http://www.kinternet.org/news/press/view/191.

KBS World. “S. Korea’s Smartphone Penetration Highest in the World at 95%.” KBS World, June 2, 2019. http://

world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=142787

Kim, Yoonhee. “검찰, 비식별 개인정보 활용 기업에 무혐의 처분.” ZDNet Korea, July 17, 2019. https://zdnet.co.kr/view/?no=20190717213635.

Lee, Jonghyun. “지금 생각해도 오싹…’개인정보보호 강화’ 10년의 역사.” Digital Daily, March 1, 2020. http://www.ddaily.co.kr/news/article/?no=192422.

Lee, Huseop. “이루다 개발사 소송 당했다… 총 2억원 손해배상 제기.” Edaily, April 1, 2021. https://www.edaily.co.kr/news/read?newsId=01590806629011856&mediaCode-No=257.

MOIS. “「개인정보 비식별 조치 가이드라인」 발간.” The Ministry of Interior and Security (MOIS), June 30, 2016. https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=55287.

Ministry of Culture, Sports, and Tourism (MCST). 2020. “데이터 경제.” Last modified March 13, 2020. https://www.korea.kr/special/policyCurationView.do?newsId=148863563.

Moon, Yong-sik. 2020. 2019 Korea Internet White Paper. National Information Society Agency (NIA).

Oh, Dae-seok, Hong, Sung-yong and Lee, Ha-yeon. “KakaoTalk in its 10th year has nearly all S. Korean population connected.” Pulse, March 2, 2020. https://pulsenews.co.kr/view.php?year=2020&no=218180.

Open Net. “March 2021 Letter to EC and EDPS on Korea’s GDPR Adequacy Review – Pseudonymized Data and Scientific Research Exemptions”. Open Net Association, April 1, 2021. http://opennetkorea.org/en/wp/3239.

Park, Sang-soo. “Moon to focus on 4th industrial revolution, smaller firms to fuel growth.” Yonhap News Agency, May 10, 2020. https://en.yna.co.kr/view/AEN20170508006300320.

PCFIR. 2020. “「2020 해커톤 규제개선 성과보고」개최.” PCFIR, December 17, 2020. https://www.4th-ir.go.kr/pressRelease/detail/1173?category=report.

PIPC. n.d. “Pseudonymization: Combination of Pseudonymized Information.” https://www.pipc.go.kr/eng/user/lgp/bnp/pseudonymization.do (Accessed July 30, 2020).

PSPD. “고객정보 3억4천여만건 무단결합 전문기관 및 20개기업 고발.” PSPD, August 11, 2017. https://www.peoplepower21.org/index.php?mid=PublicLaw&page=14&document_srl=1535215&listStyle=list.

———. 2020. “개정 개인정보 보호법 시행에 즈음한 시민사회 공동성명.” PSPD, August 4, 2020. https://www.peoplepower21.org/PublicLaw/1723330.

———. 2021. “개발’에만 치중한 AI산업육성, ‘이루다’는 예정된 참사.” PSPD, January 13, 2021. https://www.peoplepower21.org/PublicLaw/1758910.

Shim, Woomin. 2017. “개인정보 비식별 조치에 관한 입법정책적 대응과제.” National Assembly Research Service (NARS).

Shin, Yongwoo and Jeong, Joonhwa. 2021. “이루다’를 통해 살펴본 인공지능 활용의 쟁점과 과제.” National Assembly Research Service (NARS), February 15, 2021.

The Government of the Republic of Korea. 2017. *Plan for the Fourth Industrial Revolution.*

Dev Lewis

Taiwan's Covid Response

Taiwan has been praised internationally for successfully containing the local spread of COVID-19 with minimum disruption to its economy and without significant casualties (Kinling lo 2020). Despite its geographic proximity to mainland China (the first epicenter of the pandemic), and with regulatory restrictions that were the least stringent in the world (Oxford, "Oxford COVID-19 Government Response Tracker"), Taiwan reported less than 600 cases and six fatalities during the first sixteen months of the pandemic. While Taiwan is facing a tougher second wave with

14,649 cases and 635 deaths at the time of writing (Johns Hopkins University, "Coronavirus Resource Center"), there remain several lessons to learn from the Taiwanese approach, which incorporated principles of open data and bottom-up processes to its pandemic management.

Like several others, Taiwan too embraced tech applications and data driven approaches which are credited for having played an important role in its public health efforts (Wu 2021). However, the government did not default to indiscriminate mass bio-surveillance and data collection through top-down, centralised systems. It did introduce quarantine and location based contact tracing, however, it did so by working collaboratively with the civic-tech community and being transparent with the public at large (Wu 2021). In recent years, the government has experimented with the potential of technology platforms to introduce a more transparent form of working and a collaborative model of governance to build more trust in public institutions. The government leveraged the island's digital context — which ranks among the best connected societies in Asia, with 88% social media penetration (Data Reportal 2020), and is home to a community of engineers that volunteer — to use technology in the interest of public good. G0v (Gov Zero), a civic-technology group founded in 2012 has been an important part of these experiments. In the face of the deadliest global pandemic of the century, Taiwan's approach proved resilient, and can be looked

at as a model for how societies around the world can use platforms distributed towards community ownership, participatory data processes, and open-source technical solutions to tackle future challenges (Siddharth 2020).

Open data and people will build

During the start of the pandemic in January 2020, Taiwan faced a challenge that the world would eventually face in the months to come: how to provide an accessible and equitable supply of masks to the public. Mask hoarding, driven by fear of scarcity, as well as crowding at pharmacies, was a major issue during the early weeks, as mask supplies ran low (Everington 2020). To meet this challenge, Taiwan began a formal rationing of two masks, per person, per week, regulated by the National Health Insurance (NHI) card. Technology was then introduced to help implement this policy. The Taiwan government, led by Audrey Tang, Digital Minister at the Executive Yuan, worked collaboratively with g0v to create open datasets related to mask availability at National Health Insurance Administration (NHIA) approved pharmacies and health centers. These dynamic datasets, with updates at three-minute intervals, were made open access and available to developers across Taiwan to build applications and release them for public use (Yuan et al. 2020). Within days, apps were built and released. Tang announced, via Facebook, a face mask supply platform (口罩供需資訊平台) displaying several apps, that was developed by the community at large for general

public use. In total, 134 applications displaying mask availability data were recorded till date, two-thirds of which were developed by individual software developers, and two applications which were developed by governments (Taichung City Government and Taiwan Center of Disease Control; Yuan et al. 2020). Several of the most popular apps were developed by g0v members, who creatively tapped into the popular platforms in Taiwan to maximise reach and utility.

By making these datasets open to developers to create applications, the Taiwan government empowered the wider community to build a variety of applications optimised for various interfaces (web, mobile, or social media), user experiences (such as voice), and different technologies (map views, augmented reality; Yuan et al. 2020). Apart from increasing the number of choices for the public, it also distributed the network traffic load and minimised the risk of one app failing or crashing due to high traffic. For instance, Ian Chen, a g0v member, developed a bot called BuyFaceMask built on the social media platform LINE, the most popular messaging app in Taiwan. BuyFaceMask reads a user's GPS information and responds with information about the closest pharmacies and the availability of masks at each location. On the first day of use, it had 960,000 inquiries and at its peak, 2000 inquiries per minute (g0v contributors HacksMd 2020). The genesis of the entire project reflects the deep synergies between the g0v tech community and the Taiwan government.

The idea of creating this venture did not come from the government, but a citizen and g0v member named Howard Wu based in the southern city of Tainan. Howard created a mapping app to track the availability of masks using Google GPS and Places API even before the Taiwan government released the dataset. His effort was so popular that the app crashed due to the volume of traffic at launch (g0v contributors HacksMd 2020). It was at this juncture that Tang stepped in to work with Howard, and the relevant authorities, to help build the mask supply platform and dataset. This approach, where the citizen builds the specification and the government implements it, was dubbed by Audrey as “reverse procurement” — a form of iterative, bottom-up process, as opposed to a top-down government-led distribution system (Nabben 2020).

The success of these apps can be observed using relevant data. According to Google Analytics data released by the developers, after the initial peak, user traffic steadily decreased through to the end of February, suggesting less concern and panic around the availability of masks (g0v contributors HacksMd 2020). According to a small poll, 75.5% of respondents strongly agreed that they are supportive of Taiwan’s mask plan. Eventually, Taiwan was able to scale up the production of masks from two million per day in January to sixteen million in April, and the need for live maps to aid residents gradually decreased (Tai et al. 2021). Tang, while speaking at an Open Data Policy Event, said, “Col-

laboration reduces costs for everybody and it can generate unexpected applications […] in the open data and data collaborative landscape. If you open up the data, from a private-sector point of view, you attract people who improve the quality of the data" (Zahuranec 2020).

Viewed holistically, Taiwan's containment of COVID in 2020 can be put down to a range of policy interventions that rely on human effort, by volunteers and healthcare workers, as well as voluntary precautions by citizens.

A survey by the Democratic Progressive Party (DPP) in December 2020 revealed that more than 60% of the people surveyed were satisfied with the performance of President Tsai Yingwen that year (Chen 2020). A TVBS (a Taiwanese commercial television broadcasting company) poll in March 2020 revealed that 91% of the people surveyed were satisfied with the Central Epidemic Command Center (CECC), much higher than in previous years (Junhan 2020). Trust is difficult to measure and is often most conspicuous in its absence. In several societies around the world, the spread of misinformation around the virus was attributed to the lack of trust in media and institutions, a phenomenon that the WHO (2020) says contributed to an "infodemic".

More recently, the CECC has come under criticism for failing to comprehensively disclose the type of personal data collected and processed and for being unclear about the boundary of government emergency powers (Fengwu 2021). These issues

are more prominent at the time of writing, as the government is scaling up contact tracing programs to contain the second wave. However, Taiwan society today is far more resilient and has benefited from years of employing a more collaborative approach of governance, using technology.

Digital Platforms for Trust: Collaborative and open

In 2014, thousands of students and activists participated in the 'Sunflower Movement', protesting against a trade agreement between the Taiwan government (then under the Kuomintang party) and Mainland China. Tang, who was described as a self-titled 'conservative anarchist' and hacker, was among the group of protestors who believed the trade agreement was constructed in an opaque fashion and threatened Taiwan's economic and political autonomy (Siddharth 2020). After the election success of the Democratic Progressive Party (DPP) and the current President Tsai Yingwen in 2016, Tang was invited to join the government as a first-of-its-kind 'Digital Minister', to act as a bridge between all government ministries and the civic tech community to find novel ways of using technology to improve governance and rebuild the unrest in Taiwanese society that had led to the 2014 protests.

Since then, the Taiwan government has deepened its engagement with civic-tech communities, to work on important governance issues and re-imagine how citizens engage with their

government and offer their input into decision making. Central to this engagement are platforms that enable these novel interactions and allow the Taiwan government to participate in a unique blend of community engagement, trust, and data sharing.

Over the past five years, the Taiwan government and the civic tech community — with Audrey Tang as a crucial go-between — developed governance systems that can be described as deliberative processes that engage government, civil society, developers, and citizens in finding consensus around pressing governance questions with the assistance of tech platforms. One of the most influential spaces is vTaiwan, a g*0*v project run by volunteers that work with the Taiwan administration to enable public participatory policy formation and make the legislative process transparent (Tang 2016). vTaiwan has various touch points such as a website (vtaiwan.tw) and a combination of meetings and hackathons along with the consultation process. Originally aimed at internet-related regulations, it is increasingly used for a wider range of laws. Taiwan stands out as the first such platform that allows for civil society, citizens, organisations, experts, and elected representatives to participate in the process of deliberating governance questions, such as proposed laws, and help achieve a deliberative process that generates trust in solutions and outcomes (Horton 2018).

Later, a parallel space Join emerged. The Join system is a public policy participation Internet platform launched by the Taiwan National Development Council. Its aim is to make executive policy planning more open and transparent, to promote citizen participation, and to strengthen communications (Tang 2016).

Similar in design to vTaiwan, Join focuses on integrating senior career public servants into an open deliberative process with citizens. The underlying technology of both these systems is an AI platform called Pol.is. It is a digital platform for gathering and analysing diverse opinions from large groups, and producing high-level, actionable, and statistically significant insights that can be plugged into offline processes (Colin 2016). The Pol.is platform was built explicitly for the purpose of feeding on large numbers of online discussions, in the form of text comments, to build consensus and create agreements for future policy actions.

A core design feature of the Pol.is platform is that it does not allow for comments or replies.

Only three actions can be taken.

1. Agree with a statement
2. Disagree with a statement
3. Pass if unsure, with the option to write an original statement (under 140 words) for others to agree/disagree

The platform uses machine learning to take these inputs and cre-

ate a visualisation of points of agreements and disagreements through a combination of PCA (Principal Component Analysis) and k-means clustering, similar to recommendation algorithms used by Spotify and Netflix (Siddharth 2020). The underlying data is open access and fully transparent. According to Tang, "vTaiwan and Pol.is mean a rethink of the political system at the constitutional level" (Barry 2016).

Uber in Taiwan

In the last few years a number of legislative decisions have been made with significant input from deliberations on these platforms. In the four years since vTaiwan first started its operations, nearly half of Taiwan has participated, with the platform drawing 10.5 million active visitors. vTaiwan's website shows that as of August 2018, it had been used in 26 cases, with 80% resulting in "decisive government action." One of the most successful cases was the use of vTaiwan and Pol.is to regulate Uber in Taiwan, a case that reflects how these platforms work to allow consensus building among different stakeholders and allow citizens to have a say in policy making.

In 2016, the status of Uber in Taiwan was placed under the regulatory scanner. Since its entry in 2012, Uber had positioned itself as a tech company, rather than a transport company, flouting several rules that governed the traditional taxi industry, and was seen as unfair competition. vTaiwan and Pol.is were brought in to help build consensus among a variety of stakeholders rang-

ing from Uber drivers and taxi drivers, to the Taiwan Ministry of Transportation and Communication, and Uber passengers, among others. Over four weeks, 4,500 people participated and voted on 145 statements (Tang 2016). The UberX survey process asked users to begin their statements with "My feeling is…", allowing everyone to respond to each other by sharing their feelings in return, and voting on them. For example, the discussion began with this statement: "I think passenger liability insurance should be mandatory for riders on UberX private vehicles." Those responding to this statement had to decide whether they chose to agree or disagree, based on which they were divided into groups. Pol.is provided visual feedback in the form of a map which highlights areas of consensus as well as those representing non-mainstream opinion. Two groups with opposing views were then formed — although neither group represented a majority. Gradually newer statements were formed with more toned down versions in a bid to garner more support until statements that appealed to a majority were found.

After this deliberation process, an in-person discussion was held with representatives of all stakeholders present, which was live-streamed for open public access. Finally, all the Pol.is consensus items were ratified as a new regulation.

Conclusion: Taiwan model for civic-tech platforms

In a world where the platformisation of life continues at a break-

neck speed by mainly relying on big platforms to dictate information flows and access, Taiwan's experiments with more decentralised platforms, and principles of open data and transparency stand as a model for how technology platforms may be used to democratise governance and build trust in institutions.

The pandemic has exposed fault lines in societies and the friction between companies and governments in the use of technology. Taiwan's successful containment of the pandemic without significant constraining of civic liberties stands as an example for the resilience of these principles. Taiwan's own experimentation sprung from years of work by the government and civil society to rebuild trust. There are several lessons that can be learnt and methods that can be adapted from Taiwan's experience with open data and civic-tech platforms to rebuild trust using technology platforms.

References

Barry, Liz. “VTaiwan: Public Participation Methods on the Cyber-punk Frontier of Democracy.” Civic Hall, November 8, 2016. https://civichall.org/civicist/vtaiwan-democracy-frontier/.

Colin, Megill. “Pol.Is in Taiwan.” Medium, July 3, 2016. https://blog.pol.is/pol-is-in-taiwan-da7570d372b5.

Chen, Ann. “Inside the Paradise Bubble.” Logic Magazine, August 31, 2020. https://logicmag.io/care/inside-the-paradise-bubble/.

Data Reportal. “Digital 2020: Taiwan.” DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2020-taiwan (Accessed on June 29, 2021).

———. “Digital in Taiwan: All the Statistics You Need in 2021.” DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2021-taiwan.

Deck, Andrew, and Elliott, Vittoria. “How Line Built Fact-Checking into its Encrypted Messaging App.” Rest of World, March 8, 2021. https://restofworld.org/2021/how-line-is-fighting-disinformation-without-sacrificing-privacy/.

Everington, Keoni. “Taiwan’s New Mask-Rationing System Kicks in on Thursday.” Taiwan News, February 4, 2020. https://www.taiwannews.com.tw/en/news/3870428.

g0v contributors. “Questions on g0v and Taiwan Covid Success - HackMD”. https://hackmd.io/-m-WjkzJQl6tLvAD-MCWtcw?sync=&type=

Horton, Chris. 2018. “The Simple but Ingenious System Taiwan Uses to Crowdsource Its Laws.” MIT Technology Review, August 21, 2018. https://www.technologyreview.com/2018/08/21/240284/the-simple-but-ingenious-sys-

tem-taiwan-uses-to-crowdsource-its-laws/.

Jaffe, Eric. “How Open Data and Civic Participation Helped Taiwan Slow Covid.” Medium, March 27, 2020. https://medium.com/sidewalk-talk/how-open-data-and-civic-participation-helped-taiwan-slow-covid-b1449bab5841.

Johns Hopkins Coronavirus Resource Center. “Taiwan - COVID-19 Overview - Johns Hopkins”, https://coronavirus.jhu.edu/region/taiwan (Accessed June 30, 2021).

Kinling, Lo. “Taiwan’s Coronavirus Response Wins Rare Praise from WHO.” South China Morning Post, April 18, 2020. https://www.scmp.com/news/china/diplomacy/article/3080547/taiwans-coronavirus-response-wins-rare-praise-world-health.

Mask Supply Platform (口罩供需資訊平台). https://mask.pdis.nat.gov.tw (Accessed April 13, 2021).

Nabben, Kelsie. “Hacking the Pandemic: How Taiwan’s Digital Democracy Holds COVID-19 at Bay.” GCN, September 11, 2020. https://gcn.com/articles/2020/09/11/taiwan-covid-civic-hackers.aspx (Accessed April 16, 2021).

Taiwan News. “More than 60% of Taiwanese Satisfied with President Tsai’s Performance: DPP Poll | Taiwan News | 2020-12-21 15:29:00.” Taiwan News, 21 December 2020. https://www.taiwannews.com.tw/en/news/4083205 (Accessed June 30, 2021).

Schwartz, Jonathan, and Muh-Yong Yen. 2017. “Toward a Collaborative Model of Pandemic Preparedness and Response: Taiwan’s Changing Approach to Pandemics.” Journal of Microbiology, Immunology, and Infection = Wei Mian Yu Gan Ran Za Zhi 50, 2:125–32. https://doi.org/10.1016/j.jmii.2016.08.010.

Siddharth, Divya. “Taiwan: Grassroots Digital Democracy That Works.” RadicalxChange. https://www.radicalxchange.org/media/papers/Taiwan_Grassroots_Digital_Democracy_That_Works_V1_DIGITAL_.pdf (Accessed February 21, 2021).

Simons Institute. “The Digital Fence: Taiwan’s Response to COVID-19 | Simons Institute Polylogues | Simons Institute for the Theory of Computing.” https://simons.berkeley.edu/news/simons-institute-polylogues-digital-fence-taiwan-response-covid-19.

Tang, Audrey 唐鳳. “The TED Interview: How Taiwan Used Digital Tools to Solve the Pandemic with Audrey Tang on Apple Podcasts.” https://podcasts.apple.com/us/podcast/how-taiwan-used-digital-tools-to-solve-pandemic-audrey/id1437306870?i=1000477584043 (Accessed on April 9, 2021).

———. “Uber Responds to VTaiwan’s Coherent Blended Volition.” Medium, May 23, 2016. https://blog.pol.is/uber-responds-to-vtaiwans-coherent-blended-volition-3e9b75102b9b.

———. “A Thousand-Year-Old Dark Room Can Be Illuminated by a Single Lantern.” October 1, 2020. https://pdis.nat.gov.tw/en/blog/%E5%8D%83%E5%B9%B4%E6%9A%97%E5%AE%A4-%E4%B8%80%E7%87%88%E5%8D%B3%E6%98%8E/.

———. “COGOV: Rebalancing Juggling Balls of Democracy against Disinformation.” PDIS, April 17, 2020. https://pdis.nat.gov.tw/en/blog/%E5%8D%94%E5%8A%9B%E5%B0%8D%E6%8A%97%E4%B8%8D%E5%AF%A6%E8%A8%8A%E6%81%AF-%E6%B0%91%E4%B8%BB%E5%BD%A9%E7%90%83%E5%86%8D%E5%BA%A6%E9%A3%9B%E8%88%9E/.

———. “Digital Tools Open Up Taiwan’s Democratic Imaginations.” Medium, May 24, 2016. https://blog.pol.is/digital-tools-open-up-taiwans-democratic-imagina-

tions-d8f80432305c.

Tang, Audrey and Peng, Sheau-Tyng. “Open Government for Digital Health: Taiwan’s Virtual NHI Card.” PDIS, February 24, 2021. https://pdis.nat.gov.tw/en/blog/%E5%81%A5%E4%BF%9D%E5%8D%A1%E7%9A%84%E6%95%B8%E4%BD%8D%E8%BD%89%E5%9E%8B/.

———. “The Path to the Future.” PDIS, January 22, 2021. https://pdis.nat.gov.tw/en/blog/%E9%80%9A%E5%BE%80%E6%9C%AA%E4%BE%86%E7%9A%84%E6%AF%8F%E4%B8%80%E6%AD%A5/.

Tai, Yu-Lin et al. 2021. “The Effect of a Name-Based Mask Rationing Plan in Taiwan on Public Anxiety Regarding a Mask Shortage During the COVID-19 Pandemic: Observational Study.” JMIR Formative Research 5, no.1: e21409. https://doi.org/10.2196/21409.

The University of Oxford. “COVID-19 Government Response Tracker (OxCGRT).” The Oxford COVID-19 Government Response Tracker (OxCGRT), https://www.bsg.ox.ac.uk/research/research-projects/covid-19-government-response-tracker.

Quito, Anne. “Taiwan Is Using Humor as a Tool against Coronavirus Hoaxes.” Quartz. https://qz.com/1863931/taiwan-is-using-humor-to-quash-coronavirus-fake-news/ (Accessed on April 9, 2021).

Wang, C. Jason, Chun Y. Ng, and Brook, Robert. 2020. “Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing.” JAMA 323, 14: 1341. https://doi.org/10.1001/jama.2020.3151.

Wang, Junhang. “VBS Poll” Bright and beautiful anti-epidemic people feel Chen Shizhong’s satisfaction exceeds 90%,

Tsai Ing-wen sets a new high of 60% | Politics."
新頭殼 Newtalk. March 26, 2020. https://newtalk.tw/news/view/2020-03-26/381872.

WHO. "Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation." September 23, 2020. https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation.

World Economic Forum. "Agile Governance: Reimagining Policy-making in the Fourth Industrial Revolution." http://www3.weforum.org/docs/WEF_Agile_Governance_Reimagining_Policy-making_4IR_report.pdf.

Yuan, Eunice et al. 2020. "Where to Buy Face Masks? Survey of Applications Using Taiwan's Open Data in the Time of Coronavirus Disease 2019." Journal of the Chinese Medical Association, no.3(6): 557- 560, https://doi.org/10.1097/JCMA.0000000000000325.

Zahuranec, Andrew. "Summer of Open Data: Keynote Conversation with Taiwan's Audrey Tang." Medium, August 5, 2020. https://medium.com/open-data-policy-lab/summer-of-open-data-keynote-conversation-with-taiwans-audrey-tang-b6c1921e10bf.

Smitha Krishna Prasad

Covid-19 and Public Health Platforms in India

The theme of this book, “Data Opportunities and Challenges”, provokes a discussion on the role of platforms and their use of personal data within a larger context that looks beyond legal concepts and regulatory issues. The growth of Big Tech has resulted in an increasingly polarised discourse around the use of personal data.

Our experiences with Covid-19 offer a rare perspective on the conversation about data. Over the past year and a half, we have seen much controversy across the world as governments and the tech industry came together to build platforms aimed at en-

abling us to respond to the pandemic better. These platforms initially came in the form of contact tracing applications, quarantine and crowd trackers, telemedicine providers and even simple public health information providers. More recently though, there has been a shift towards platforms that enable registrations for vaccines, and immunity / vaccine passports.

Underlying these efforts was an already increasingly important discussion on health data and the digitalisation of health services and records to ease access to medical and pharmaceutical services across service providers and locations. These initiatives come with several questions around the harmonisation/ standardisation of data, aggregation, anonymisation, security, accuracy, privacy etc. Each of these points of friction can be categorised as both a challenge and an opportunity in how we learn to deal with personal health information. On the issue of security alone, we have seen several instances over the past few years when the consequences of moving health services and records to online-only models posed a risk not only to the privacy of patients but also to their physical well-being (Ikeda 2021). Covid-19 has only escalated many of these issues.

This piece will look at the Indian experience in building public health platforms in response to the Covid-19 pandemic — focusing on the opportunities that were available and utilised, the risks that came with the use of personal information of millions of people, and equally the use of platforms that excluded access

to millions — in the context of the local regulatory environment.

The Covid-19 Platforms: Contact tracing and beyond

Aarogya Setu, the Indian government's contact tracing application, has been the most discussed technological tool in India's response to the Covid-19 pandemic by far. The application was built in a matter of days and released for public use in the early days of the pandemic in India (Indian Press Information Bureau 2020; Punj 2020). The application's primary function is to enable digital contact tracing, by means of a combination of self-assessments by users and always-on Bluetooth and GPS tracking (Tandem Research 2020). In addition, the location data collected by the application allows government authorities to identify emerging hotspots and take steps towards containing the spread of the virus. The application's functions were also expanded to allow the publication of healthcare bulletins, and today the app interfaces with the government's vaccine registration portal.

Similar to the Singapore experience (Goggin 2020), the application, which was released in early April 2020, was promoted by the government and was reportedly one of the fastest growing apps in the world at the time (Mehrotra 2020). The use of the application was also made mandatory in many instances at the time of its release, by both the government (at central, state and domestic levels in different cases) and private sector actors (for

instance, employers requiring employees to download and use the application). This in turn raised many questions about the need for such an app, the potential for exclusion given that the application was only available to smartphone users, the security and protection of personal data collected by the app, the regulatory framework (or lack thereof) backing the mandates for the use of the app, and the 'volunteers' from the private sector who built the app. Concerns around these questions were further exacerbated as the government indicated that Aarogya Setu would become foundational to India's plans to build a national health stack — a controversial plan to digitise India's healthcare infrastructure (Krishna Prasad 2020; Agrawal 2020).

In addition to Aarogya Setu, several other applications and platforms — both public and private sector initiatives — were launched to help combat the Covid-19 pandemic. Among the public platforms, the most popular were quarantine monitoring applications, self-assessment applications that allow users to assess the risk of contracting Covid-19, and platforms that were meant to provide information, and advisories. Some states also built applications to ease permissions for essential workers to move around freely when the country was in lockdown. Many of these user-facing platforms required personal information to be submitted at the time of registration, and in many cases at several intervals during the use of the platform. For instance, the Quarantine Watch application implemented by the state of

Karnataka reportedly required users to send in selfies showing their location every hour to indicate that they were not breaking quarantine rules (Deccan Herald 2020). Researchers reported that in many cases there was no specific or clear privacy policy governing the use of personal information collected and processed by the platforms (Tandem Research 2020; Bedi and Sinha 2020). Given that it was often mandatory for certain sections of the population to use some of these platforms, privacy and security concerns were common in discussions around many of these platforms.

Public Health and Data: The regulatory frameworks

In order to understand the evolution of digital public health platforms, and the challenges that arose as the country responded to the Covid-19 pandemic, it is relevant to discuss the existing regulatory frameworks that govern both public health services and digital platforms. These frameworks can be broken up into two broad buckets for the purpose of this article — those around existing frameworks for public health initiatives, particularly in the context of communicable diseases and epidemics, and those around informational privacy and the digital world.

Epidemics and Public Health

The Indian public health system is not new to the idea of collection and use of data towards improving public health facilities and responding to epidemic prone diseases. The National Cen-

tre for Disease Control has been running an Integrated Disease Surveillance Program (IDSP) for over 15 years, with the aim of "strengthening disease surveillance … by establishing a decentralise State based surveillance system for epidemic prone diseases to detect early warning signals," and ensuring that the country can respond to health challenges (NCDC 2021). While these systems have been digitised in parts since 2007, the Integrated Health Information Platform, which houses the data entry and management systems for the IDSP was initially tested in 2018 and officially launched only in 2021 (Ministry of Health and Family Welfare 2021). The development of these programs suggests that there have been consistent efforts towards implementing policy frameworks for collection and management of data in our public health disease surveillance systems. However, there is little documentation to indicate how privacy and security concerns with regard to any personal information that may be collected and used will be handled — both pre and post digitisation.

The legislative framework that has guided India's response to the Covid-19 pandemic provides little solace in this regard. The two legislations that governed this response were the Epidemic Diseases Act, 1897 and the Disaster Management Act, 2005.

The Epidemic Diseases Act 1897, is meant to enable better prevention of the spread of dangerous epidemic diseases. However, the law itself betrays its colonial roots with its lack of specificity

or accountability. This law simply empowers State governments to take any special measures required to prevent the outbreak or spread of a dangerous epidemic disease. The few details in the provisions under the law clearly suggest that such measures are meant to be more in the nature of increasing the policing powers of the State rather than taking measured action in the interest of public health.

The Disaster Management Act, 2005 on the other hand, is relatively recent, and sets out administrative structures and procedures to be followed by various levels of government in preparing for and responding to disasters. However, the term disaster is defined very broadly, to mean:

> catastrophe, mishap, calamity or grave occurrence in any area, arising from natural or man made causes, or by accident or negligence which results in substantial loss of life or human suffering or damage to, and destruction of, property, or damage to, or degradation of, environment, and is of such a nature or magnitude as to be beyond the coping capacity of the community of the affected area.

The more specific provisions of the law that discuss disaster response in terms of relief camps and re-building of infrastructure for instance, also suggest that the law was perhaps not meant to deal with prolonged public health emergencies such as a pandemic.

Platforms and Privacy

Information privacy and surveillance have been the focus of technology related public policy discourse in India for several years now, as a result of both the global phenomena that is big tech and local developments, particularly in the public sector in India. Between controversies around Aadhaar (the biometric-based national digital identity system) and more recent initiatives around facial recognition and AI in the public sector, and incidents of data breaches such as Cambridge Analytica and others in the private sector, it has become clear to all stakeholders that there is a need for a comprehensive data protection law in India.

However, at the time of writing, we have to make do with the limited protections offered under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("IT Rules"), issued under the Information Technology Act, 2000. The IT Rules largely apply to the collection and processing of "sensitive personal data and information," including physical, physiological and mental health condition, medical records and history, and biometric information by private companies. Even in this context, the protections offered are limited, and easily overwritten by standard form contracts.

Over the past year or so, a more comprehensive legislative frame-

work in the form of the Personal Data Protection Bill, 2019 has been widely discussed. This bill is currently being examined by a parliamentary committee, which will provide its recommendations on the bill. While the bill has been lauded as a step forward in India's journey towards enacting comprehensive data protection legislation, there are several debatable issues even in the last published version of the document.

The bill does consist of a few provisions that are specifically relevant to healthcare/ public health concerns. The bill considers health data to be sensitive, and affords additional protections to health data, defined to mean, "data related to the state of physical or mental health of the (individual) and includes records regarding the past, present or future state of the health of such (individual), data collected in the course of registration for, or provision of health services, data associating the (individual) to the provision of specific health services." The bill also takes medical or public health emergencies into account and provides an exception to the requirement for consent before the collection or processing of personal information in such situations.

It also allows the government to exempt research activities from provisions under the law, if required, under specific conditions that ensure that there is no risk of significant harm to the individual. While it is clear, especially now since the onset of the Covid-19 pandemic that there is value in using certain types of data for research in the public interest, the provision for research

exemptions under the bill is quite broad. It allows the authorities to exempt any entities (private or public sector), from any or all requirements under the law without exception, and offers little guidance on the parameters to be met in such situations.

Public Digital Health Policies and Systems

India's National Health Policy, 2017 published by the Ministry of Health and Family Welfare, discusses the need to leverage digital technology to improve healthcare services in the country. Among other things, it envisages the establishment of a National Digital Health Authority, and an "integrated health information system which serves the needs of all stake-holders and improves efficiency, transparency, and citizen experience." The policy suggests that a federated national health information architecture can be implemented, potentially using Aadhaar as an identification tool. It also suggests building registries to enable enhanced public health/big data analytics, create a health information exchange platform, and a national health information network.

Over the past four years we have seen several initiatives that aim to implement this policy, starting with the National Health Stack (NHS), which aims to build nationally shared digital infrastructure usable by both Centre and State across public and private sectors. The National Health Stack strategy document published in 2018, also envisaged the creation of unique digital health IDs to enable users to avail the services that the NHS

enables.

When a large number of healthcare services moved online as a result of the Covid-19 pandemic, it was suggested that these digital tools — including Aarogya Setu, the contact tracing application — could be foundational to the implementation of the National Health Stack.

In July 2020, the National Health Authority published the National Digital Health Mission's (NDHM) strategy overview document, which aims to significantly improve the efficiency, effectiveness, and transparency of health service delivery overall. The NDHM devotes an entire section to the management of health data. For this purpose, it envisions a federated and standardised health record exchange, with digital consent tools meant to empower users. The NDHM works on the underlying assumption that the Personal Data Protection Bill, 2019 will be the governing legislative framework for this purpose. The NDHM also notes the importance of a standardised process of identification, and recommends a Digital Health ID, while stating clearly that the same will not be mandatory to avail healthcare services. A Health Data Management Policy was subsequently published for consultation in August 2020, and approved in December 2020.

These strategies and policies aim to build a public digital healthcare system that connects public and private healthcare providers throughout the country, leveraging technology and data,

while maintaining individual health records in a secure, privacy-friendly manner. While a granular discussion on the pros and cons of each of these documents is beyond the scope of this piece, it is important to note that they often do not clarify basic questions such as the availability of technical infrastructure and know-how, or institutional capacity for implementation (Desai 2020). This raises several concerns since research suggests that many initiatives along these lines, including an ongoing effort to promote the standardisation and use of Electronic Health Records with origins back to 2013, have faced challenges due to a lack of infrastructure and capacity (Rathi 2019).

Controversies and Opportunities

At the time of writing this article, reports suggest that the use of many of these platforms may be mandated once again as the country grapples with a second wave of Covid-19 cases (Ghosh 2021). However, the most relevant platform at this time is the CoWIN portal which is being used to manage vaccine distribution in the country. The platform, which is currently only available via browsers, and not through an independent mobile application, allows individuals to register for Covid-19 vaccines, find vaccination centres and availability near their location, and schedule an appointment. Citizens also have the option of registering for a vaccine through the Aarogya Setu app, or simply walking into vaccination centres (in the case of certain age groups, and other categories). For walk-ins the staff at the vac-

cination centre log their details onto the CoWIN platform at their end. Once vaccinated, a certificate indicating the same is issued in a digital format, also available through the same platform.

As we move into this next phase, it is important to reflect on the developments of the past year and understand what learnings have already been considered, and what more should perhaps be taken into account.

The push by the central and/or state governments in India for the use of many of these platforms, and the mandatory requirements to use them in many cases bring up several points of friction. First, there are questions about the very nature of the solutions they aim to provide and whether it is backed by good science. The next question that arises is whether these platforms based on digital technology are the right or only way to deliver these solutions.

A number of the issues in this context revolve around questions of accessibility, inclusion and discrimination — a majority of Indians are either not connected to the Internet, or do not have smartphones (Kak and Joshi 2020). In addition, there are many instances where phones are shared between family members, people face problems with network/internet connectivity in remote areas, or areas where government mandated internet shutdowns have been imposed. Apart from smartphone usage and internet penetration, concerns have been raised in relation

to the use of specific tech-based tools. For instance, in the early days of the pandemic, Aadhaar numbers were mandatory for access to Covid-19 testing. And when the government started discussing vaccine rollout plans, once again there was talk of linking vaccinations to Aadhaar-based identification systems. For the purpose of this article, we will explore the concerns raised in relation to the use of data collected for and processed in relation to the platforms used as a part of the Indian government's response to Covid-19. While it is important to collect and process data for the purpose of treating patients and making evidence-based policy decisions — there are inherent risks in any indiscriminate collection and use of data. These risks range from the personal harm that a breach of privacy can cause when personal data is used, to the larger public harms that can occur when the quality of data used for scientific research or policy making is compromised. Pushing out hastily built solutions in the interest of addressing a crisis may end up causing more long-term harm than good by potentially increasing surveillance capacities of the State and the private sector, and institutionalising ham-fisted tech solutions.

In the past year, various governments in India have gone down the path of implementing mandatory requirements for the use of platforms before rolling the same back due to challenges around legal backing, and concerns around exclusion, access, privacy and security among others. In the case of Aarogya Setu,

the government first amended the privacy policy attached to the application after issues were raised around the use of personal data. When concerns were raised regarding the lack of legal backing for the roll out of such a platform, the Aarogya Setu Data Access and Knowledge Sharing Protocol was drafted and implemented (by executive order) to "ensure secure data collection by the Aarogya Setu mobile application, protection of personal data of individuals, and the efficient use and sharing of personal or non-personal data for mitigation and redressal of the COVID-19 pandemic" (Aarogya Setu Data Access and Knowledge Sharing Protocol 2020). This protocol was meant to restrict access to the data collected by Aarogya Setu to government agencies and public health research institutions for the purpose of formulating a health response. However, responses to Right to Information requests suggest that no official records have been maintained regarding the sharing of Aarogya Setu data (Das 2020). More recently, it was revealed that some data has been shared with police forces in Jammu and Kashmir (Das 2021).

As of April 2021, India was considering a 'touchless' vaccination system that is based on verification of Aadhaar details using facial recognition technology. Limited availability of vaccines, and the potential need for 'vaccine passports' (although controversial) may justify the need to ensure verification and recording of the identity of individuals obtaining the Covid-19 vaccine. At the

time of writing, citizens are able to get vaccinated with any valid ID. The linking of vaccination drives to facial recognition technology is not the first suggestion the Indian government has made regarding the expansive and controversial use of facial recognition technology. However, the impact, whether on questions of access and discrimination, or privacy and surveillance will be far reaching and potentially irreparable, if made mandatory, at a time when the country has no effective data protection law, is grappling with vaccine shortages, and a devastating second wave of Covid-19 cases.

At the core of the problems that arise from the use of tech platforms discussed in this article, is the lack of good regulation and policy, and the transparency, accountability and oversight that should be implemented as a result. As seen in the sections above, there is a desperate need for cohesive, human rights-respecting regulation and /or updates to existing law in multiple contexts, including pandemic/epidemic response and public health, privacy and data protection, and perhaps even in the parameters for reactive policy and rule making in emergency like situations.

To the extent that this relates to the collection and processing of data, there is need for legislative and policy measures that enable individuals to exercise their fundamental human rights, with due consideration to specific public health needs that may arise. This means that the law should ideally establish parame-

ters regarding the kind of data that is required and processed in different circumstances:

1. an individual patient is symptomatic or found to be suffering from Covid-19 and requires treatment
2. contact tracing needs to be undertaken and quarantine/isolation requirements need to be enforced to curtail the immediate spread of the disease
3. scientific research on how the virus spreads and the impact it has needs to be undertaken in order to identify treatments and vaccines from a public health perspective
4. research is required to understand the manner in which the country's public health infrastructure needs to be improved to deal with epidemics/pandemics in the future

Each of these circumstances may require the use of different data sets, as well as different formats of data. They may also require that the collection and processing of such data be undertaken by different stakeholders — doctors, hospitals, researchers, different agencies of the government, and in certain cases even private sector stakeholders.

Where personal data is being used, identifying such circumstances acts as a first step towards ensuring purpose limitation, one of the most important principles of personal data protection. This exercise will also help determine the circumstances under which exceptions will need to be made to the standard/comprehensive data protection law in the case of a medical emer-

gency, or a public health emergency, or research in the public interest. Appropriate conditions can then be built in for such exceptions, incorporating well accepted principles that ensure that any incursions on human rights are limited, necessary and proportionate to the need at hand.

Consultative, open exercises to determine the kinds of technology and data use that is necessary could also go a long way in ensuring that the most secure and adaptive standards be put in place to ensure that data is accurate, of a quality that is beneficial, and recorded and maintained in a harmonised manner. Digital infrastructure where required, can be built on this basis.

References

Agrawal, Aditi. "Aarogya Setu Will Include Telemedicine, Greater Personalisation; May Act as Building Block for India Health Stack." MediaNama (blog), April 22, 2020. https://www.medianama.com/2020/04/223-aarogya-setu-upcoming-features/

Bedi, Pallavi, and Amber Sinha. 2020. "A Survey of Covid 19 Apps Launched by State Governments in India." The Centre for Internet and Society, July 14, 2020. https://cis-india.org/internet-governance/blog/a-survey-of-covid-19-apps-launched-by-state-governments-in-india.

Das, Saurav. "EXCLUSIVE | Govt Ignores Its Own Vital Safeguards on Aarogya Setu." TheQuint, October 30, 2020. https://www.thequint.com/news/india/exclusive-govt-fails-to-implement-its-own-data-protection-safeguards-under-aarogya-setu-protocol.

"#BREAKING Our Fears Have Come True, at Least on Record. I Can Now Confirm That at Least One State Government Has Shared People's Aarogya Setu Data with a Law Enforcement Agency. Jammu & Kashmir's Kulgam District Has Done so with the Kulgam Police. 1/3 Https://T.Co/V4hdFx3P5z." Tweet. @OfficialSauravD (blog), March 30, 2021. https://twitter.com/OfficialSauravD/status/1376809695566909444.

Deccan Herald. "Privacy of Quarantined Protected in Selfie App." Deccan Herald, April 1, 2020. https://www.deccanherald.com/state/top-karnataka-stories/privacy-of-quarantined-protected-in-selfie-app-820217.html.

Desai, Arpitha. 2020. "Comments to the National Health Authority on the Draft Health Data Management Policy." Centre for Communication Governance at National Law University Delhi, September 22, 2020.

Ghosh, Poulomi. "Karnataka Brings Back 'Quarantine Watch' App, Hand Stamping, as Covid Cases Rise." Hindustan Times, March 25, 2021. https://www.hindustantimes.com/india-news/karnataka-brings-back-quarantine-watch-app-hand-stamping-as-covid-cases-rise-101616691572892.html.

Goggin, Gerard. 2020. "COVID-19 Apps in Singapore and Australia: Reimagining Healthy Nations with Digital Technology." Media International Australia, August, 2020, https://doi.org/10.1177/1329878X20949770.

Ikeda, Scott. "Rise in Healthcare Data Breaches Driven by Ransomware Attacks." CPO Magazine, March 18, 2021. https://www.cpomagazine.com/cyber-security/rise-in-healthcare-data-breaches-driven-by-ransomware-attacks/

Indian Press Information Bureau. "Backend Code of Aarogya Setu Released in Open Domain." November 20, 2020. pib.gov.in/Pressreleaseshare.aspx?PRID=1674492.

Kak, Amba, and Divij Joshi. "India's Digital Response to COVID-19 Risks Inefficacy, Exclusion and Discrimination." The Caravan, April 19, 2020. https://caravanmagazine.in/health/india-digitial-response-covid-19-risks-inefficacy-exclusion-discrimination.

Krishna Prasad, Smitha. "Aarogya Setu App Lacks Clear Legal Backing and Limits, Tends towards Surveillance." Deccan Herald, May 9, 2020. https://www.deccanherald.com/specials/sunday-spotlight/aarogya-setu-app-lacks-clear-legal-backing-and-limits-tends-towards-surveillance-835692.html.

Mehrotra, Karishma. “Behind Aarogya Setu App Push: ‘At Least 50% People Must Download for Impact.’” The Indian Express (blog), April 11, 2020. https://indianexpress.com/article/coronavirus/behind-aarogya-setu-app-push-at-least-50-people-must-download-for-impact-6357121/

Ministry of Health and Family Welfare. “Dr Harsh Vardhan Launches Integrated Health Information Platform (IHIP), the Revised next Generation Integrated Disease Surveillance Programme (IDSP) Digital Platform.” April 5, 2021, pib.gov.in/Pressreleaseshare.aspx?PRID=1709676.

National Centre for Disease Control. “Integrated Disease Surveillance Program”. https://www.ncdc.gov.in/index1.php?lang=1&level=1&sublinkid=143&lid=54

Punj, Vivek.“‘Aarogya Setu Made with Industry, Academia’: Centre Clarifies after RTI Opens Can of Worms.” Business Today, October 28, 2020. https://www.business-today.in/current/economy-politics/aarogya-setu-jointly-developed-with-industry-academia-centre-clarifies-after-rti-opens-can-of-worms/story/420199.html.

Rathi, Ayush. 2019. “Is India’s Digital Health System Foolproof?” Economic and Political Weekly, November, 7–8.

Tandem Research. 2020. “Tech Tools For COVID-19.” https://www.techtoolsforcovid19.in/

“The Aarogya Setu Data Access and Knowledge Sharing Protocol.” 2020.

This is a translation of Recent Debates on Data Utilisation and Protection: 3 Data Laws and Lee Luda (KOR), provided by Kelly Kim

김가연
(사)오픈넷

최근의 데이터 활용과 보호 논의: 데이터 3법과 이루다

서론
한국 인터넷과 플랫폼의 역사

스마트폰 보급률 세계 1위인 한국(KBS World 2019)은 미국 다음으로 (폐쇄적인 중국을 예외로 하면) 토종 플랫폼이 선전하는 나라일 것이다. 구글에 맞서 네이버가, 페이스북의 왓츠앱에 맞서 카카오톡이, 아마존에 맞서 쿠팡이 압도적인 점유율을 자랑하고 있다. 지금은 명실상부한 인터넷 강국이지만 1980년대까지만해도 한국의 정보통신 기반은 열악했다. 그러나 1982년 5월 15일 한국전자기술연구소(KIET, 현 ETRI)와 서울대학교 간 SDN(System Development Network)이 구축되면서 한국은 미국에 이어 세계 2번째, 아시아 1번째로 TCP/IP에 기반한 인터넷을 개발한 나라가 되었다(Chon et al 2005). SDN 개발을 주도한 전길남 박사는 '한국 인터넷의 아버지'로 불리며, 2012년 ISOC 인터넷 명

예의전당에 헌액되었다.

이후 1994년에 한국통신(KT)이 상용 인터넷서비스 '코넷(KORNET)'을 개시했고, 1997년에는 인터넷 이용자 100만명을 돌파했다. 1998년 두루넷이 상용 초고속인터넷 서비스를 개시한 1년 만인 1999년에는 인터넷 사용자 1000만명을 돌파했다. 인터넷 개발 20년만인 2001년 한국은 경제협력개발기구(OECD)가 발표한 초고속인터넷 보급률 세계 1위를 기록했다(문용식 2020, 13). 한국은 1996년 세계 최초 CDMA 이동전화 상용서비스를 개시하고, 1998년에 이동전화 가입자 1000만명을 달성한 나라이기도 하다. 이런 눈부신 발전이 가능했던 배경에는 좁은 국토와 높은 인구밀도도 한 몫 했지만 무엇보다 정부의 적극적인 정보화 정책 추진과 학교와 연구기관을 중심으로 한 민간의 자발적 참여가 큰 역할을 했다고 할 수 있다.

이러한 인프라를 바탕으로 1990년대 중반 수많은 벤처기업들이 생겨나면서 한국 플랫폼의 역사가 시작되었다. 1995년, 중앙일보는 아시아 최초로 인터넷 신문 서비스를 시작했다. 1996년에는 인터넷 쇼핑몰 인터파크가 서비스를 개시하고 넥슨에서 세계 최초 그래픽 머드(MUD, Multi User Dungeon) 게임 '바람의 나라'를 출시했다.[1] 1997년에는 다음커뮤니케이션에서 한메일 서비스, 삼성SDS 사내 벤처 1호 네이버가 한글 검색엔진을 출시했다. 상용 초고속인터넷 서비스가 시작된 1998년에는 엔씨소프트가 대규모 다중사용자 온라인 롤플레잉 게임(MMORPG, Massively Multiplayer Online Role Playing Game) '리니지' 서비스를 시작했다.

상용 초고속인터넷 서비스의 등장으로 1990년대 후반 한국 플랫폼이 폭발적으로 늘어났다. 1999년 국내 최초 포털사이트 다음이 오픈했고,

1 바람의 나라는 2010년 9월 세계 최초의 상용화 그래픽 MMORPG로 기네스북에 등재되었고 2011년에는 가장 오랫동안 서비스된 그래픽 MMORPG로 다시 기네스북에 올랐다.

국내 첫 인터넷 뱅킹 서비스가 시작되었고, 세계 최초 웹 기반 채팅서비스 세이클럽이 등장했다. 그리고 한국 기술로 개발된 세계 최초 인터넷 전화 서비스(VoIP, Voice over Internet Protocol) '다이얼패드'가 먼저 미국에서 무료로 서비스를 시작했으며, 검색엔진 '엠파스'가 서비스를 개시하고 네이버와 경쟁을 시작했다. 2000년에는 페이스북보다 4년 빨리 사진 등을 공유하는 SNS 싸이월드가 서비스를 개시했다. 2004년에는 인터넷 이용자 3000만명을 돌파했으며, 2005년에는 한국 온라인 게임 시장 규모가 1조원을 돌파했다(안정배, 강경란 2014, 200). 유튜브가 설립된 2005년에 한국에서는 1인 방송 플랫폼 아프리카TV가 서비스를 개시했고, 2010년에는 모바일 메신저 카카오톡이 출시되었고 출시 이후 계속 메신저 앱 점유율 1위를 차지하고 있다(Oh, Hong, and Lee 2020).[2]

한국 플랫폼이 직면한 데이터 기회와 도전

한국의 플랫폼이 직면한 데이터 기회와 도전은 다시 말하면 데이터의 활용과 보호 사이의 긴장이라고 할 수 있다. 데이터는 4차 산업혁명 시대의 필수 자원으로 원유에 비교되기도 한다. 인공지능·빅데이터·클라우드컴퓨팅 같은 최근의 정보통신기술(ICT)과 그에 기반한 제품과 서비스 생산에는 데이터가 필수적이다. 2017년 취임한 문재인 대통령의 4차 산업혁명 정책과 디지털 뉴딜 정책의 핵심에는 데이터 활용이 있다. 반면, 모든 국민에게 태어날 때부터 고유식별변호를 부여하는 주민등록제도, 휴대폰실명제, 인터넷실명제와 같은 개인정보 수집을 의무화하는 정책, 프라이버시 침해에 둔감한 문화 등이 맞물려 크고 작은 개인정보 유출 사고가 수없이 일어났으며, 개인정보 보호 강화 요구는 계속 커졌다. 그 일환으로 한국에서는 GDPR 제정 훨씬 전인 2011년 개인

2 카카오톡은 출시 10주년을 맞은 2020년 한국 인구의 87%(약45백만명)가 사용하는 앱이며, 2018년 기준 메신저 앱 점유율 99.2%을 차지했다.

정보보호법이 제정되고 개인정보보호위원회가 설립되었으며, 최소한 제도적으로는 세계에서 가장 엄격한 개인정보보호법제를 갖고 있는 나라 중 하나라고 할 수 있다. 이에 자유로운 데이터 활용을 원하는 산업계와 프라이버시 침해를 우려하는 이용자와 시민사회, 그리고 이를 조율해야 하는 국가 간 갈등이 계속되어 왔다. 이러한 갈등은 2020년 데이터 활용에 중점을 둔 "데이터3법"의 입법 과정에서 특히 부각되었다. 아래에서는 한국의 데이터 관련 법과 정책, 이해관계자의 입장을 간단히 소개하고, 최근 한국에서 데이터 활용과 보호 사이의 갈등의 주요 쟁점들이 부각된 인공지능 챗봇 "이루다" 사례를 살펴보고 그 시사점을 도출해보기로 한다.

데이터3법과 빅데이터 정책

2020년 데이터 3법 개정

2020년 개정된 "데이터3법"은 개인정보보호법, 정보통신망 이용촉진 및 정보보호에 관한 법률(이하 "정보통신망법"), 신용정보의 이용 및 보호에 관한 법률(이하 "신용정보법")을 말한다. 데이터의 활용에 중점을 둔 데이터3법은 발의될 때부터 찬반 논란이 많았던 법이다. 보호와 활용은 반비례하므로, 데이터 활용만 중시하고 개인정보 보호는 약화시킬 것이란 우려가 있었기 때문이다. 그럼에도 불구하고 데이터3법은 우여곡절을 거쳐 2020년 1월 9일 국회를 통과했으며, 2020년 8월 5일부터 시행됐다.

데이터3법 중 가장 중요한 법은 개인정보보호법이다. 2011년 제정된 개인정보보호법은 1994년에 제정된 '공공기관의 개인정보보호에 관한 법률'을 그 연원으로 한다.[3] 개인정보보호법이 제정되기 전에는 민간 분

3 한국에서 개인정보보호법이 공공 분야에 먼저 도입된 이유는 80년대 후반 시작된 행정전산망의 구축과 깊은 관련이 있다. 행전전산망 구축 사업과 국가주요업무의 전산화 확대는 행정 부문의 완전한 정보화를 가능하게 한 반면, 개인정보 부당사용 또는 무단유출로 인한 사생활 침해 등 각종 부작용이 우려되었던 것이다.

야의 개인정보 보호가 법적 사각지대에 놓였었다. 인터넷 활성화와 함께 개인정보의 중요성이 대두되며 개인정보보호법이 탄생했다. 데이터 3법 중 신용정보법은 1995년 제정됐는데, '신용정보'와 '개인신용정보'에 대한 개념을 도입하고 신용정보를 취급하고자 하는 사업자는 금융위원회의 허가를 받거나 신용정보와 무관한 정보를 수집·조사하지 못하도록 하는 등의 내용을 담았다. 정보통신망법은 데이터3법 중 가장 오래된 법으로, 1986년 제정된 '전산망 보급 확장과 이용촉진에 관한 법률'이 근간이다. 하지만 개인정보와 관련한 규정이 포함된 것은 1999년 정보통신망법으로 개정되면서부터이다.

한국의 개인정보 보호의 역사는 역설적으로 개인정보 침해의 역사라고 할 수 있다. 2008년 1월 해킹으로 인해 옥션 이용자 1800만명의 개인정보가 유출됐다. 개인정보보호법이 제정된 2011년에는 네이트와 싸이월드를 운영하던 SK컴즈의 데이터베이스가 해킹되면서 3500만명의 개인정보가 유출됐다. 같은 해 넥슨에서도 약 1300만명의 개인정보가 유출되는 사고가 발생했다. 2014년에는 대형 보안사고가 연달아 터졌다. KB국민·NH농협·롯데 카드 3사 개인정보 유출 사고가 그것이다. 당시 카드 3사에서 유출된 개인정보는 한국 인구의 2배인 1억400만건에 달한다. 그리고 카드 3사 개인정보 유출이 발생한지 3개월 만에 KT 홈페이지 해킹으로 1200만명의 개인정보가 유출됐다(이종현 2020). 잇따른 개인정보 유출로 개인정보 보호 필요성의 목소리가 커지면서 2016년 보호 강화를 목적으로 한 법 개정이 이루어졌다. 징벌적 손해배상제도와 형사처벌 조항을 도입하는 등 개인정보처리자에 대한 규제를 대폭 강화했다. 하지만 그로부터 다시 4년의 시간이 흘렀고 데이터 활용을 요구하는 목소리가 높아지며 분위기가 반전됐다. 특히 전세계적으로 빅데이터와 AI 등 데이터에 기반한 4차 산업혁명의 흐름에 주목한

정부와 국회는 데이터의 활용에 중점을 둔 데이터3법 개정을 추진하게 되었다.

가명정보 도입과 가명정보 처리 가이드라인

데이터3법 개정의 가장 중요한 내용은 '가명정보'에 관한 것이다. 개정된 개인정보보호법은 GDPR을 참고하여 가명정보 개념을 도입했다. "가명정보"란 가명처리를 한 개인정보로서 "원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보"이며(제2조 1호 다목), 이때 "가명처리"란 "개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것"을 의미한다(제2조 1호의2). 한편, 개인정보보호법은 "가명정보 처리에 대한 특례"를 규정하여, 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있도록 하고 있다(제28조의2). 특히 과학적 연구 목적의 경우 "기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구"(개인정보보호위원회, 연도미상)라고 규정함으로써 데이터를 기반으로 하는 새로운 기술·제품·서비스 개발 등에 개인정보를 활용할 수 있는 길을 열었다. 이처럼 가명정보를 정보주체의 동의 없이 활용할 있도록 하는 것이 이번 데이터3법의 핵심이라고 할 수 있다. 2020년 8월 데이터3법이 시행되자 개인정보보호위원회는 2020년 9월 '가명정보 처리 가이드라인'을 발표했다. 가이드라인은 크게 개인정보처리자가 개인정보를 활용하여 가명처리를 수행하기 위한 절차를 안내하는 "가명처리," 다른 개인정보처리자 간의 가명정보의 결합 및 반출에 관한 절차를 안내하는 "가명정보의 결합," 그리고 가명정보에 대한 관리적, 기술적, 물리적 보호조치에 관한 사항을 안내하는 "가명정보의 안전한 관리" 세 장으로 나뉜다.

4차 산업혁명과 빅데이터 정책

2017년 취임한 문재인 대통령은 취임 전부터 4차 산업혁명을 강조했으며(Park 2017) 취임 후 100대 국정과제 경제 전략으로 "과학기술 발전이 선도하는 4차 산업혁명"을 내세웠다(청와대, 연도미상). 과학기술정보통신부에게 4차 산업혁명의 인프라 구축과 규제 개선 책임을 맡기고 대통령 직속 4차산업혁명위원회를 신설했다. 과제의 주요 내용에는 "데이터 개방 및 유통 활성화"가 포함되었다.

4차 산업혁명은 인공지능, 빅데이터 등 디지털기술로 촉발되는 초연결 기반의 지능화 혁명으로 산업뿐만 아니라 국가시스템, 사회, 삶 전반의 혁신적 변화를 유발한다(대한민국 정부 2017, 16). 4차 산업혁명은 D.N.A.(데이터, 네트워크, 인공지능) 등의 지능정보기술을 기반으로, 다양한 기술, 분야, 산업과 융합해 국가사회 전반에 파괴적 혁신을 일으키고 있다. 4차 산업혁명은 과거 '정보화'가 차지했던 영역을 인공지능 기반의 '지능화'로 업그레이드하는 것이다. 따라서 4차 산업혁명의 성공 여부는 인공지능 수준과 직결되며, 인공지능은 빅데이터의 영향을 크게 받는다. 결국 빅데이터는 4차 산업혁명의 산출물이자 동시에 추동력이다(정준화 2018, 2). 대통령 직속 4차산업혁명위원회(이하 "4차위")는 급변하는 환경 속에서 특정 부처에서만 다루기 힘든 4차 산업혁명 관련 아젠다를 심의·조정하고 관련 혁신을 촉진하기 위해 만들어졌으며, 2020년부터는 '국가 데이터 정책 컨트롤 타워'로서 역할을 부여받아, 데이터 기반 디지털 경제 활성화에 역량을 집중하고 있다. 이러한 배경 하에 현 정부에서 데이터3법 개정이 이루어지게 된 것이다.

데이터3법 개정 전인 2016년, 정부는 빅데이터 활성화를 위해 '개인정보 비식별 조치[4] 가이드라인'을 발표했다. 그간 업계에서는 비식별 조

4 '비식별화'는 특정 정보로부터 '개인 식별 가능성'을 제거하는 조치 및 과정을 의미하며, 종종 이러한 용어는 '익명화'와 동일한 의미로 사용된다. 비식별화라는 용어는 미국 등의 국가에서 주로 활

치 기준이 명확히 제시되지 않아 빅데이터 활용에 어려움이 많다고 호소해 왔다. 또한, 학계와 언론에서는 빅데이터, IoT 등 새로운 IT 기술과 융합 산업의 발전에 따른 데이터 이용 수요에 대응하기 위해 가이드라인이 필요하다는 의견을 꾸준히 제기해 왔다. 이에 정부는 기업의 불확실성을 제거하여 산업 발전을 도모하는 한편, 데이터 이용 과정에서 개인정보 침해 방지를 위한 비식별 조치 가이드라인을 만든 것이다(행정안전부 2016). 가이드라인은 개인정보의 비식별 조치 기준, 활용범위 등에 대해 규정하면서, 기업이 보유한 고객의 정보를 한국인터넷진흥원(KISA) 등 전문기관을 통해 다른 기업이 보유한 정보와 결합할 수 있게 했다. 통신3사를 비롯한 국내 20개 기업은 비식별 조치 전문기관을 통해 3억 4,000만 건에 달하는 개인정보를 결합해 활용했다. 하지만 2017년 11월 참여연대 등 시민사회단체들은 KISA 등 전문기관과 기업들을 모두 개인정보보호법 위반으로 고발했다(참여연대 2017). 이후 사건은 검찰에서 무혐의 처리되었으나(김윤희 2019) 이로 인해 기업들은 소극적이 되었고 가이드라인은 사실상 사문화되었다.

데이터3법을 둘러싼 다양한 이해관계자들과 입장

개정 전 데이터3법은 소관 부처가 각각 다르고 유사·중복 조항이 많았기 때문에 개인정보 관련 문제가 발생했을 때 일관된 대응이 어려웠다. 공공과 민간을 규율하는 개인정보보호법은 행정안전부와 개인정보보호위원회, 금융권을 규율하는 신용정보법은 금융위원회, 정보통신 사업자를 규율하는 정보통신망법은 방송통신위원회 소관이었다. 데이터3법 개정을 통해 정보통신망법은 개인정보보호 관련 사항 전반을 개인정보보호법을 이관했다. 주체도 방송통신위원회에서 개인정보보호위원회로 변경했다. 신용정보법 역시 개인정보보호법과 유사·중복 조항

용되고 있으며, 익명화 또는 익명가공이라는 용어는 EU 및 일본 등지에서 활용되고 있는 것으로 파악되지만, 대체적으로 두 용어가 혼용되고 있는 양상이다(심우민 2017, 2).

을 정비하고 금융분야 빅데이터 분석·이용의 법적 근거를 명확히 했다. 또한 행정안전부 산하에 있는 것과 다름없었던 개인정보보호위원회의 독립성과 위상을 강화하여, 중앙행정기관으로 격상했다.

한편 그동안 현 정부의 정책 기조는 개인정보의 보호보다는 활용을 강조하는 모습을 보였다. 앞서 언급했듯이 문재인 대통령은 당선 전부터 4차 산업혁명을 강조했으며, 4차위는 개인정보 보호와 데이터 활용 이슈를 1차, 2차, 3차 해커톤 의제로 다뤄 데이터3법 개정을 이끌어낸 주역이다(4차위 2020). 문대통령은 2018년 8월 31일 '데이터 경제로의 전환'을 선언했으며 이에 맞춰 정부는 데이터 경제 활성화를 위한 산업 육성과 데이터 활용 관련 규제혁신 계획을 발표했다(문화체육관광부 2020). 또한 2020년 7월 정부는 디지털 뉴딜을 핵심으로 하는 한국판 뉴딜 정책을 발표했다. 디지털 뉴딜 정책의 핵심인 "디지털 댐"은 "데이터 수집·가공·거래·활용기반을 강화하여 데이터 경제를 가속화하고 5세대 이동 통신(5G) 전국망을 통한 전(全)산업 5세대 이동 통신(5G)·인공지능(AI) 융합 확산"을 목표로 한다(청와대, 연도미상).

산업계는 지속적으로 개인정보 보호 규제를 완화하고 데이터 활용을 가능하게 해줄 것을 요구했다. 특히 네이버, 카카오와 같은 플랫폼 기업들의 목소리가 컸다. 2018년 10월경 국회 과학기술정보방송통신위원회 국정감사에서 김범수 카카오 의장은 "카카오브레인의 대표를 하면서 카카오의 비전과 대한민국의 미래를 위해 필요한 인재를 모았는데, 30% 밖에 확보하지 못했다. 이들은 국내에 남지 않는 이유를 데이터의 수집과 활용이 어려운 구조라고 하였다."고 하며, "AI기술은 데이터를 활용하는 경험이 많을수록 발전할 수밖에 없다, 골든타임을 놓치면 과학기술의 미래는 어둡다."고 강조했다(이설영 2018). 2019년 한국인터넷기업협회, 코리아스타트업포럼, 한국게임산업협회 등은 한국의 인터

넷 기업들이 4차 산업혁명 시대를 주도하기 위해서는 “개인정보 보호”와 “안전한 데이터 활용”을 포용할 수 있는 기술 중립적 법제의 정비가 시급하다고 강조하면서 데이터3법의 조속한 입법을 촉구한 바 있다(한국인터넷기업협회 2019).

반면 개인정보 보호 강화를 지속적으로 주장해 온 시민사회는 데이터3법의 통과를 줄곧 반대했으며, 데이터3법을 ‘개인정보 도둑법’이라고 부르며 개선을 요구하고 있다. 특히 가명정보와 관련하여, ‘과학적 연구’의 범위가 불분명하고, 기업들의 가명정보 판매를 저지할 수 있는 수단이 없고, 가명정보의 결합과 결합물의 반출을 허용하도록 한 것에 대해 문제를 제기했다(참여연대 2020).

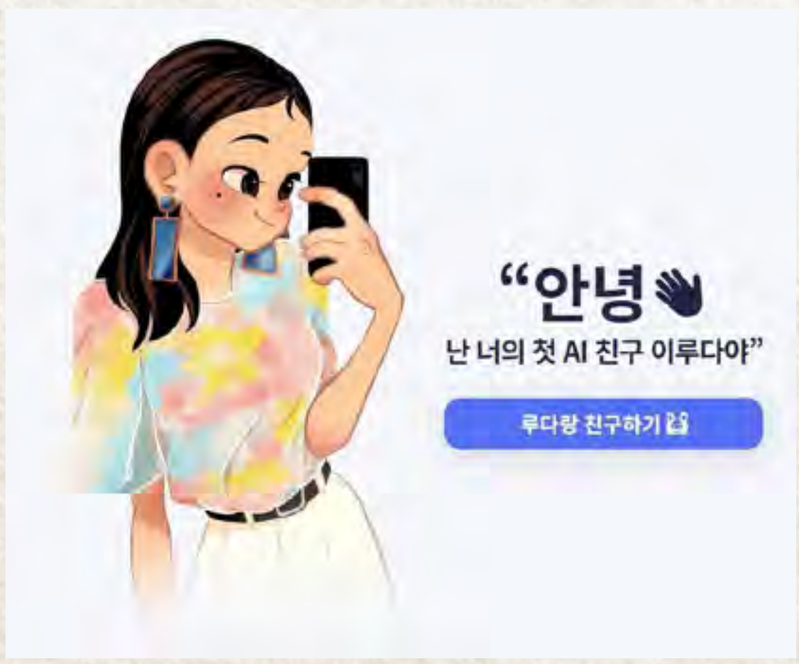
오픈넷은 가명정보의 동의 없는 처리를 가능하게 하는 ‘과학적 연구’ 목적에 있어 GDPR처럼 연구가 공유될 필요가 있으며, 가명정보에 대해서 열람권 등 정보주체의 권리를 박탈하고 있는 조항의 개정이 필요함을 계속 주장해왔다(오픈넷 2020). 시민사회는 정부가 2020년 7월 발표한 디지털 뉴딜 정책에 대해서도 정부가 데이터를 산업 육성의 관점에서만 보고 있으며 ‘국민의 사생활’을 팔아 경제성장하겠다는 것이라고 신랄하게 비판했다(진보네트워크센터 2020).

‘이루다’에 비춰 본 AI와 데이터3법

‘이루다’ 사례 개요

데이터3법 개정으로 힘을 얻을 대표적인 산업은 AI이다. AI는 4차 산업혁명과 데이터 경제의 핵심 산업이며, 민간뿐만 아니라 정부 차원에서도 AI에 대한 투자를 아끼지 않고 있다. 이런 흐름에서 인공지능 챗봇 ‘이루다’ 사례는 인공지능의 윤리와 프라이버시 보호 등 인공지능에 관한 최근 쟁점을 모두 내포하는 중요한 사례로 살펴볼 가치가 있다.

2020년 12월 23일 출시된 이루다는 스캐터랩(Scatter Lab)에서 개발한 인공지능 챗봇(AI chatbot) 서비스이다. “안녕, 나는 너의 첫 AI 친구 이루다야”라는 캐치프레이즈를 건 이루다는 20세 여대생이라는 가상 프로필을 가지고 있었고 페이스북 메신저와 인스타그램에서 친구로 추가할 수 있었다. 이루다는 사람들의 실제 대화를 기반으로 프로그래밍 되었기 때문에 자연스러웠고 일상의 모든 주제에 대해서 대화할 수 있었다. MZ 세대들은 실제 친구와 대화하는 것처럼 느껴지는 이루다에 열광했고 서비스 2주 만에 40만명 이상의 가입자를 확보할 정도로 인기를 끌었다. 그런데 MS 챗봇 테이와 같이, 처음에는 이루다가 사용한 차별⊠혐오표현들이 문제되었다. 다음으로 이름, 주소 등 개인정보 유출 논란이 일어나고, 학습 데이터 수집과 활용 과정에서 개인정보보호법을 위반했다는 지적이 제기되었다(참여연대 2021). 결국 이루다에 대한 인식은 급격히 악화되었고, 출시 20일 만에 서비스를 전면 중지하게 되었다. 개인정보보호위원회는 KISA와 함께 1월 조사에 착수했으며, 4월 28일 스캐터랩에 대해 개인정보보호법 위반을 이유로 총 1억 330만원의 과징금과 과태료 등을 부과했다(최홍석 2021). 또한 3월에는 245명의 이용자가 스캐터랩을 상대로 개인정보 침해에 대한 집단소송을 제기했다(이후섭 2021).



이루다 홈페이지 화면

이루다 사례의 쟁점은 크게 두 가지로 나뉜다. 첫 번째는 인공지능의 윤리와 편향성 문제이고, 두 번째는 개인정보보호법 위반 문제이다.

이 중 첫 번째 문제는 이 글의 주제와 관련이 적기 때문에 두 번째 문제를 자세하게 검토한다.

‘이루다’의 개인정보 관련 쟁점

개인정보 수집에 대한 동의. 개인정보위원회의 조사에 의하면 스캐터랩은 자사가 제공하는 앱 서비스인 ‘텍스트앳’과 ‘연애의 과학’에서 수집한 카카오톡 대화를 이루다의 인공지능 개발과 운영에 이용했다. 둘 다 카카오톡 대화 내용을 분석해서 상대방의 호감도를 파악하고 연애 상담을 해주는 서비스이다. 스캐터랩은 약 60만명의 이용자의 카카오톡 대화 문장 94억여 건을 이용했으며, 이루다 서비스 운영 과정에서 20대 여성의 카카오톡 대화문장 약 1억 건을 응답 DB로 구축했다. 스캐터랩은 개인정보처리방침에서 ‘신규 서비스 개발에의 활용’을 명시하고 동의를 받았기 때문에 이러한 데이터 이용이 적법하다고 주장했다. 이에 대해 개인정보보호위원회는 1) ‘텍스트앳’과 ‘연애의 과학’ 개인정보처리방침에 ‘신규 서비스 개발’을 포함시키고 이용자가 로그인함으로써 동의한 것으로 간주하는 것만으로는 이용자가 ‘신규 서비스 개발’ 목적의 이용에 동의했다고 보기 어렵고, 2) ‘신규서비스 개발’이라는 기재만으로 이용자가 ‘이루다’ 개발과 운영에 카카오톡 대화가 이용될 것을 예상하기도 어려우며, 3) 이용자의 개인정보자기결정권이 제한되는 등 이용자가 예측할 수 없는 손해를 입을 우려가 있어 스캐터랩이 개인정보를 수집하면서 적법한 동의를 받지 않았고 이용자의 개인정보를 수집한 목적을 벗어나 이용했다고 판단했다.

개인정보의 가명처리 또는 비식별 조치. 이루다의 대화 중에 이름, 주소 등이 노출됨에 따라 학습데이터에 대한 가명처리가 적절히 이루어졌는지 논란이 되었다. 스캐터랩은 데이터가 비식별화 절차를 거쳤으며 개별적이고 독립적인 문장 단위로 이루어져 있어 개인을 식별할 수 없다고 밝혔다. 하지만 비정형적인 일상 대화의 맥락 상 비식별화되지 않은 정보들이 남아 있었던 것이다. 이에 대해 시민사회는 데이터3법이 자초한 문제라며 비판했다. 이루다처럼 기업들이 개인정보를 가명처리만 하면 정보주체의 동의 없이 서비스 개발에 무한대로 이용할 수 있게 허용했다는 것이다(참여연대 2021). 구체적으로는 GDPR은 연구가 공유되는 공익적인 '과학적 연구'의 경우에 정보주체의 동의 없이 가명정보를 이용할 수 있게 하지만, 데이터3법은 기업의 상업적 이용을 위해서도 동의 없이 가명정보를 이용할 수 있게 했다는 것이다(오픈넷 2021). 또한 개인정보보호위원회의 '가명정보 처리 가이드라인'은 대화내용과 같은 비정형 데이터의 가명처리 기준으로 사용하기에는 부족하다는 지적도 있다(신용우, 정준화 2021, 3). 아쉽게도 개인정보보호위원회는 학습데이터가 적절하게 가명처리되었는지, 동의가 필요 없는 가명정보의 이용에 해당하는지에 대해서 판단하지는 않았다. 다만 스캐터랩이 GitHub에 이름 등이 포함된 카카오톡 대화문장 1,431건과 함께 인공지능 모델을 게시한 것에 대해 가명정보를 불특정 다수에게 제공하면서 "특정 개인을 알아보기 위하여 사용될 수 있는 정보"를 포함했다는 이유로 개인정보보호법 제28조의2 제2항을 위반한 것이라고 판단했다.

개선방향

스캐터랩이 정보주체로부터 개인정보 수집에 대한 동의를 받았다고 주장했지만 개인정보보호위원회의 제재를 받은 주된 이유는 그 동의가 형식적이었기 때문이다. 형식적인 동의 제도는 정보주체의 개인정보자

기결정권을 보장하기보다 개인정보 수집 및 활용의 정당화의 수단으로 남용될 수 있다. 따라서 동의 제도를 단순화·실질화하여 실효성을 높이고, 사후통제를 강화할 필요가 있다. 특히 인공지능은 웹크롤링·사물인터넷과 같은 신기술을 이용하여 사람의 개입 없이 자동으로 개인정보를 수집·활용할 수 있기 때문에 사전동의와 사후통제의 적절한 병행이 중요하다. 그리고 가명정보의 동의 없는 처리를 허용하는 "과학적 연구"의 범위가 명확하게 정의되어야 한다. 다음으로, 가명처리의 경우 일상대화, 영상과 같은 비정형 데이터의 재식별 위험성을 평가하고 방지할 수 있도록 가이드라인을 개선하고 기술·방법론에 관한 연구를 추진할 필요가 있다. 이를 위해서는 까다로운 가명처리의 절차적 요건이 간소화되어야 한다. 가명처리는 연구·개발뿐만 아니라 개인정보 보호에도 바람직하기 때문이다. 가명처리는 GDPR이 장려하는 보안조치이자 프라이버시 중심 디자인으로 기능한다. 마지막으로, 인공지능의 경쟁력은 학습데이터 확보에 있다. 그러나 많은 중소기업·스타트업은 충분한 데이터를 확보하기 어렵고, 가명처리를 할 여력도 충분하지 않다. 따라서 이에 대한 정부의 지원을 강화할 필요가 있다.

결론

세계 최고 수준의 ICT 인프라를 바탕으로 눈부시게 성장한 한국의 플랫폼이 현재 마주하는 가장 큰 마찰은 데이터 보호의 영역에서 일어나고 있다. 자유로운 데이터 활용을 요구하는 산업계와 프라이버시 침해를 우려하는 이용자와 시민사회, 그리고 이를 조율해야 하는 국가 간의 갈등이 계속되어 왔으며, 데이터 3법의 입법 과정에서 각 이해관계자들은 첨예하게 대립했다. 이루다는 이러한 갈등이 현실화된 구체적인 사례를 제공하고 개선방향을 생각해보게 해주었다. 데이터의 보호와 활용은 서로의 안티테제가 아니다. 모든 이해관계자들은 프라이버시 보호를

기반으로 안전한 활용이 이루어질 수 있게 합리적인 법·제도를 만들어 가는 노력을 지속해야 할 것이다.

참고문헌

4차산업혁명위원회. 2020. "「2020 해커톤 규제개선 성과보고」 개최." 4차산업혁명위원회, December 17, 2020. https://www.4th-ir.go.kr/pressRelease/detail/1173?category=report.

개인정보호위원회. 연도미상. "개인정보 가명처리·가명정보 결합." [검색 2021.7.30.]. https://www.pipc.go.kr/np/default/page.do?mCode=D040010000

김윤희. 2019. "검찰, 비식별 개인정보 활용 기업에 무혐의 처분." ZDNet Korea. July 17, 2019. https://zdnet.co.kr/view/?no=20190717213635

대한민국 정부. 2017. 4차 산업혁명 대응계획. 대한민국 정부.

문용식. 2020. 2019 한국인터넷백서. 한국정보화진흥원(NIA).

문화체육관광부. 2020. "데이터경제." [최종수정 2020.3.13.]. https://www.korea.kr/special/policyCurationView.do?newsId=148863563

신용우, 정준화. 2021. "'이루다'를 통해 살펴본 인공지능 활용의 쟁점과 과제." 국회입법조사처. February 15, 2021.

심우민. 2017. 개인정보 비식별 조치에 관한 입법정책적 대응과제. 국회입법조사처.

안정배, 강경란. 2014. 한국 인터넷의 역사. ㈜블로터앤미디어.

오픈넷. 2020. "데이터3법의 아이러니 - 공공목적 없이 정보주체의 권리를 제한하는 개인정보보호법 제28조의7 재개정을 요구한다." 오픈넷. September 25, 2020. https://opennet.or.kr/18822

———. 2021. "오픈넷, EU에 대한민국 GDPR 적정성 평가시 가명정보특례조항에 대한 검토 요구." 오픈넷. March 30, 2021. https://

opennet.or.kr/19560.

이설영. “김범수 ‘AI 인재유출 심각… 문제는 데이터 규제.’” 파이낸셜뉴스. October 14, 2018. https://www.fnnews.com/news/201810141713094687.

이종현. 2020. “지금 생각해도 오싹…’개인정보보호 강화’ 10년의 역사.” 디지털데일리. March 1, 2020. https://www.ddaily.co.kr/news/article/?no=192422.

이후섭. 2021. “이루다 개발사 소송 당했다… 총 2억원 손해배상 제기.” 이데일리, 2021.4.1. https://www.edaily.co.kr/news/read?newsId=01590806629011856&mediaCodeNo=257.

정준화. 2018. “4차 산업혁명 시대의 빅데이터 정책과제.” 국회입법조사처. July 4, 2018.

진보네트워크센터. 2020. “디지털뉴딜, ‘국민사생활’ 팔아 경제성장하겠다는 것.” 진보네트워크센터. July 21, 2020. https://act.jinbo.net/wp/43213/

참여연대. 2017. “고객정보 3억4천여만건 무단결합 전문기관 및 20개기업 고발.” 참여연대, 2017.8.11. https://www.peoplepower21.org/index.php?mid=PublicLaw&page=14&document_srl=1535215&listStyle=list.

———. 2020. “개정 개인정보 보호법 시행에 즈음한 시민사회 공동성명.” 참여연대, 2020.8.4. https://www.peoplepower21.org/PublicLaw/1723330.

———. 2021. “‘개발’에만 치중한 AI산업육성, ‘이루다’는 예정된 참사.” 참여연대, 2021.1.13. https://www.peoplepower21.org/PublicLaw/1758910.

청와대. 연도미상. “한국판 뉴딜 대한민국 대전환의 시작.” [검색 2021.7.30.] https://www1.president.go.kr/KNewDeal.

———. 연도미상. “국정과제” [검색 2021.7.30]. https://www1.president.go.kr/government-projects#page2.

최홍석. 2021. “개인정보위, ‘이루다’ 개발사 ㈜스캐터랩에 과징금·과태료 등 제재 처분.” 개인정보보호위원회. April, 2021. https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298.

한국인터넷기업협회. 2019. “인기협 등 5개 단체, 국회에 개인정보보호법 개정안의 조속 처리 촉구.” 한국인터넷기업협회. 26 September, 2019. http://www.kinternet.org/news/press/view/191.

행정안전부. “「개인정보 비식별 조치 가이드라인」 발간.” 행정안전부. June 30, 2016. https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=55287.

Chon, Kilnam et al. 2005. “A Brief History of the Internet in Korea.”한국 인터넷 역사 프로젝트 [Korea Internet History Project]. August 29, 2005. https://sites.google.com/site/koreainternethistory/publication/brief-history-korea-eng-ver%20(%20Accessed%20July%2030,%202021).

KBS World. “S. Korea’s Smartphone Penetration Highest in the World at 95%.” KBS World. June 2, 2019. http://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=142787.

Oh, Dae-seok, Hong, Sung-yong and Lee, Ha-yeon. 2020. “KakaoTalk in its 10th year has nearly all S. Korean population connected.” Pulse. March 2, 2020. https://pulsenews.co.kr/view.php?year=2020&no=218180.

Park, Sang-soo. 2020. “Moon to focus on 4th industrial revolution, smaller firms to fuel growth.” Yonhap News Agency. May 10, 2020. https://en.yna.co.kr/view/AEN20170508006300320

Contributors

Kelly Kim

Kelly Kim is General Counsel at Open Net Association. Open Net is a non-profit, civil society organisation founded in 2013 to defend and promote Internet freedom and digital rights. She focuses on issues regarding freedom of expression online, privacy and mass-surveillance, intermediary liability and Internet governance. She also actively engages in international discussions regarding digital rights including the UN Internet Governance Forum.

Dev Lewis

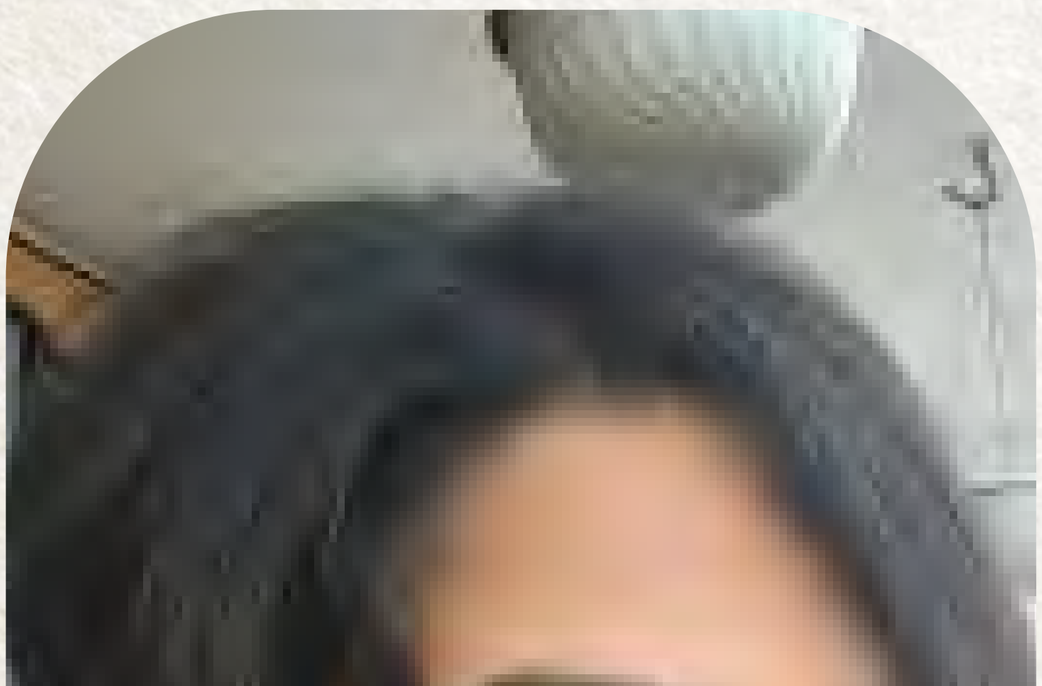
Dev Lewis is a Fellow and Program Lead at Digital Asia Hub, where his work looks at the intersections of technology, politics, and society in China and the wider region. Dev was a Yenching Scholar at Peking University where he graduated with a Masters in China Studies, and has a degree in International Relations from Roger Williams University. He frequently writes for several regional publications and think tanks, as well as ChinaIndia Networked, a newsletter he started to interpret Chinese media for a global audience. Dev is presently also a Global Governance Futures 2035 Fellow with GPPi in Berlin.

Smitha Krishna Prasad

Smitha Krishna Prasad is a Assistant Professor of Law at the National Law School of India University, and a Senior Research Fellow at the Digital Asia Hub. Her primary research interests focus on issues around privacy, data protection and surveillance, as well as questions of emerging technology and law, and the expansion of tech regulation through legal and economic policy making initiatives. At the Digital Asia Hub, she is involved in research related to the governance of platforms, and more broadly digital infrastructure used to deliver public services. Previously, Smitha was a Director at the Centre for Communication Governance at National Law University, Delhi, where she led the Centre's research, policy and capacity building work on technology law and policy developments in India. She has also worked with the Technology, Media and Telecoms practice at Nishith Desai Associates. Smitha holds an LL.M. degree in International Legal Studies from the New York University School of Law, as well as a B.A.LL.B. from Symbiosis Law School, Pune.

Gayatri Khandhadai

Gayatri Khandhadai is a lawyer with a background in international law and human rights, international and regional human rights mechanisms, research, and advocacy. She previously worked with national and regional human rights groups, focusing on freedom of expression. Her current focus is on digital rights and policy in Asia with specific emphasis on freedoms of expression, religion, assembly and association on the internet.



Nishant Shah

Nishant Shah is a Professor of Aesthetics and Cultures of Technology at ArtEZ University of the Arts and an endowed professor at Radboud University in the Netherlands. He is a Faculty Associate at the Berkman Klein Centre for Internet & Society, Harvard University, USA and also a research mentor with the Feminist Internet Research Network. He is a knowledge partner on art-rights-technology-society programming with the Dutch Human Rights organisation HIVOS. Nishant's work is at the intersection of digital technologies, social and future justice, gender and sexual equity, and cultural expressions, with a particular focus on non-canonical geographies and bodies. He is a feminist, humanist, and technologist and his new book Really Fake (University of Minnesota Press) is now available for Open Access.

Copyeditor and proofreader: Shruthi Menon

Graphic design: Angie Kang

Colophon

Title of Book: Small Books for Big Platforms

Title of Series: Book 2 – Data Opportunities and Challenges

Published 2021, by the **Digital Asia Hub**, and the Professorship Aesthetics and Cultures of Technology at **ArtEZ University of the Arts**.

Series Editors: Nishant Shah, Malavika Jayaram, and Vincent Zhong

Volume Contributors: Kelly Kim, Dev Lewis, Smitha Krishna Prasad, Gayatri Khandhadai, Nishant Shah

Primary Knowledge Partner: Nishant Shah

Copyeditor and proofreader: Shruthi Menon

Cover and Design: Angie Kang

Available for Open Access in digital formats.

For more information or queries contact: n.shah@artez.nl, mjayaram@digitalasiahub.org