GLOBAL INFORMATION SOCIETY WATCH 2019

Artificial intelligence:
Human rights, social justice and development

Association for Progressive Communications (APC),
Article 19, and Swedish International Development Cooperation Agency (Sida)

Global Information Society Watch

2019

APC Sida ARTICLE 19

Global Information Society Watch 2019
Artificial intelligence: Human rights, social justice and development

Operational team
Valeria Betancourt (APC)
Alan Finlay (APC)
Mallory Knodel (ARTICLE 19)
Vidushi Marda (ARTICLE 19)
Maja Romano (APC)

Project coordination team
Valeria Betancourt (APC)
Cathy Chen (APC)
Flavia Fascendini (APC)
Alan Finlay (APC)
Mallory Knodel (ARTICLE 19)
Vidushi Marda (ARTICLE 19)
Leila Nachawati (APC)
Lori Nordstrom (APC)
Maja Romano (APC)

GISWatch 2019 advisory committee
Namita Aavriti (APC)
Rasha Abdul Rahim (Amnesty International)
Alex Comninos (Research ICT Africa)
Malavika Jayaram (Digital Asia Hub)
J. Carlos Lara (Derechos Digitales - América Latina)
Joy Liddicoat (Centre for Law and Emerging Technologies, University of Otago)
Andrew Lowenthal (EngageMedia)
Micaela Mantegna (Geekylegal/Machine Intelligence Lab, Center for Technology and Society, San Andres University)
Valeria Milanes (Asociación por los Derechos Civiles)

Project coordinator
Maja Romano (APC)

Editor
Alan Finlay (APC)

Assistant editor and proofreading
Lori Nordstrom (APC)

Publication production support
Cathy Chen (APC)

Graphic design
Monocromo

Cover illustration
Matías Bervejillo

We would like to extend a special note of thanks to a number of authors who have made ad honorem contributions to this edition of GISWatch. We gratefully acknowledge the following:

Philip Dawson and Grace Abuhamad (Element AI)
Anita Gurumurthy and Nandini Chami (IT for Change)
Rasha Abdul Rahim (Amnesty International)

APC would like to thank the Swedish International Development Cooperation Agency (Sida) and ARTICLE 19 for their support for Global Information Society Watch 2019.

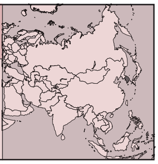
Published by APC
2019
Printed in USA

Global Information Society Watch 2019 web and e-book
ISBN 978-92-95113-13-8
APC Serial: APC-201910-CIPP-R-EN-DIGITAL-302

Disclaimer: The views expressed herein do not necessarily represent those of Sida, ARTICLE 19, APC or its members.

KOREA, REPUBLIC OF

DATA PROTECTION IN THE AGE OF BIG DATA IN THE REPUBLIC OF KOREA



Korean Progressive Network Jinbonet
Miru
https://www.jinbo.net

Introduction

The Korean government is currently focusing on developing emerging technologies, such as artificial intelligence (AI), the "internet of things" (IoT) and "big data", as part of the so-called Fourth Industrial Revolution. These technologies are interconnected in that deep-learning technology needs big data to train AI, and a vast amount of data, including personal data, is produced through IoT devices. With the development of these technologies, privacy and data protection issues have also been raised. Although the Korean government has recognised data protection as a critical policy issue, the government has continued to implement policies focused on the utilisation rather than protection of personal data.

Policy background and brief history

Personal data protection laws in Korea

Before establishing the Personal Information Protection Act (PIPA)[1] in 2011, there were several acts for regulating personal data in different sectors. The PIPA was enacted to protect personal data covering all areas of society, but even after passing the PIPA, existing acts still remain, such as the Act on Information and Communication Network Utilization (Network Act) and the Credit Information Use and Protection Act (Credit Act). Accordingly, there are several supervisory bodies that govern each act, such as the Ministry of the Interior and Safety (MOIS) which governs the PIPA, the Korea Communications Commission (KCC) which governs the Network Act, and the Financial Service Commission (FSC) which governs the Credit Act, as well as the Personal Information Protection Commission (PIPC) established according to the PIPA. The diffusion of supervisory bodies and acts causes confusion for data subjects and controllers and hinders the establishment of a unified data protection policy. In addition, these bodies are government ministries, so they have no independence from the government, and the PIPC does not have enforcement powers.[2]

Guidelines for De-identification of Personal Data[3]

There has been constant debate in recent years over whether and under what conditions personal data could be processed further beyond the original purpose. Industry keeps requesting permission for utilising personal data for big data analysis and development of AI. As an answer to this, the previous government announced the "Guidelines for De-identification of Personal Data"[4] in June 2016. According to the guidelines, the de-identification of personal data refers to a "procedure to remove or replace all or part of an individual's identifiable elements from the data set to prevent the individual from being recognized."[5] Because de-identified personal data is no longer considered personal data, it can be processed without the consent of data subjects for purposes other than the original purpose, such as big data analysis, and even provided to third parties. In addition, the guidelines allow companies to combine customers' de-identified personal data with that of other companies through designated authorities. However, the guidelines were criticised for having no legal basis, because there was no concept of "de-identification" in the PIPA. Moreover, de-identified data is at risk of being re-identified, and as government was aware of these risks, it prohibited disclosing de-identified data to the public.

Since the publication of the guidelines, 20 companies have de-identified customer data and combined the data sets with those of other companies through designated agencies, which amounted to 340 million entries as of August 2017. In opposition to the guidelines, civil society organisations, including the Korean Progressive Network Jinbonet, have laid criminal charges with the prosecutor

[1] www.law.go.kr/lsInfoP.do?lsiSeq=142563&chrClsCd=010203&urlMode=engLsInfoR&viewCls=engLsInfoR#0000

[2] https://act.jinbo.net/wp/38733

[3] https://www.kisa.or.kr/public/laws/laws2_View.jsp?cPage=1&mode=view&p_No=282&b_No=282&d_No=3&ST=T&SV=

[4] https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000827254&fileSn=0

[5] Ibid.

against the relevant companies and designated agencies for violating the PIPA.[6]

Policy hackathon on the use and protection of personal data in the age of big data

In 2018, the current government held a "policy hackathon" – or a multistakeholder discussion forum[7] – on the use and protection of personal data in the age of big data in order to solve this issue through the amendment of the PIPA. The policy hackathon was attended by stakeholders from industry, civil society, academia and the government. They gathered to reach a social consensus on major issues related to the Fourth Industrial Revolution. Through two hackathon meetings, broad agreements were reached. The participants agreed to use the concepts of personal data, pseudonymised data and anonymised data, borrowed from the European Union's General Data Protection Regulation (GDPR), instead of the ambiguous concept of de-identification. In this context, pseudonymised data refers to the data processed to make it difficult to directly identify a natural person without combining it with other information. However, it is still personal data because it can be re-identified when combined with other information. On the other hand, anonymised data, such as statistical results, is data processed so that a specific individual can no longer be identified.

Since the hackathon was a place for discussion and interaction, but was not a place to decide policies, there was still a task for government ministries to formulate policies reflecting the hackathon's agreements and to revise relevant laws in the National Assembly.[8]

Three big data laws

In November 2018, the so-called "three big data laws",[9] including the amendments to the PIPA, were proposed in the National Assembly to ease regulation on personal data protection for the purpose of revitalising the big data industry. The three big data laws, however, promote the sale and sharing of personal data instead of protecting it. In addition, the PIPA amendments undermine the rights of data subjects and reduce the data processor's obligation to protect personal data. As a result, civil society is against the three big data laws and is again calling for legislation to protect personal data. You can read more detail on this in the section on "Issues around the amendment of the PIPA" below.

Two cases on the use of de-identified data for big data analysis

From 2011 to 2014, The Korea Pharmaceutical Information Center (KPIC) sold the details of 4.7 billion prescriptions for medication to IMS Health Korea[10] for KRW 1.6 billion (USD 138,368).[11] KPIC provided the software used for health insurance claims, PM2000, to drugstores. By using PM2000, KPIC collected and sold the information of patients' diseases and medication claims without permission.[12] No one who received prescription drugs at a drugstore during the period was aware of this.

In 2015, a joint government investigation team on personal data crimes charged IMS Health Korea for violating the personal data of patients. However, the company is claiming innocence. It insists that because the resident registration numbers (RRNs), which can identify specific patients for each prescription, were de-identified through encryption, this data was not personal data.[13] However, researchers from Harvard University, Latanya Sweeney and Ji Su Yoo, published a paper proving that the encryption method used in the case could be easily decrypted, meaning that individuals could be re-identified.[14]

In 2015, the Health Insurance Review and Assessment Service (HIRA), which is run by the state, sold the medical data of 1.1 million hospitalised patients to KB Life Insurance for "insurance product research". Even prior to this, the HIRA had sold the data of elderly patients to Samsung Life for the purpose of "research" to calculate insurance premiums and develop new insurance products in 2011. Although medical data is considered sensitive data, the HIRA never acquired consent from the patients for using the data. It insisted that the data sets it

[6] https://act.jinbo.net/wp/33555

[7] The policy hackathon was hosted by the Presidential Committee on the Fourth Industrial Revolution and aims to reach an agreement through full-day discussions among stakeholders on critical social issues.

[8] Chamsesang. (2018). *A Survey on Data Protection and Human Rights in the Age of the Fourth Industrial Revolution.* National Human Rights Commission of the Republic of Korea. https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=001003001004&pagesize=10&boardtypeid=16&boardid=7603678

[9] The "three big data laws" mean the PIPA amendments, Credit Act and Network Act. Credit Act: https://elaw.klri.re.kr/kor_service/lawView.do?hseq=46276&lang=ENG; Network Act: https://elaw.klri.re.kr/kor_service/lawView.do?hseq=25446&lang=ENG

[10] IMS Health is an international company for data analysis of health care data. The company's name was recently changed to IQVIA. IMS Health Korea is the Korean branch of the company. https://www.iqvia.com/about-us

[11] www.monews.co.kr/news/articleView.html?idxno=85001

[12] www.hani.co.kr/arti/economy/it/752750.html

[13] https://act.jinbo.net/wp/39218

[14] Sweeney, L, & Yoo, J. S. (2015, 29 September). De-anonymizing South Korean Resident Registration Numbers Shared in Prescription Data. *Technology Science.* https://techscience.org/a/2015092901

sold were not personal data because the HIRA de-identified them by encrypting or deleting the RRNs and patient names.[15]

Issues around the amendment of the PIPA

The range of use of pseudonymised data

Although hackathon participants agreed to use the concepts of personal data, pseudonymised data and anonymised data instead of the ambiguous concept of de-identification contained in the guidelines, they failed to reach an agreement on the scope of the use of pseudonymised data.[16] Nevertheless, the amendment allows the use and provision of pseudonymised data for "statistics, scientific research and archiving purposes in the public interest" without consent from data subjects (Article 28-2). Here, scientific research includes commercial research. In addition, as with the guidelines for the de-identification of personal data, the amendment allows the combining of data sets from data controllers through designated specialised agencies (Article 28-3).

The Korean government insists that the amendment of the PIPA makes it the equivalent of the GDPR, which also allows further processing of personal data beyond the original purpose of collection under certain conditions for scientific research purposes. However, the amendment allows extensive use of personal data in comparison to the GDPR, while safety measures to protect personal data are meagre.

Firstly, the amendment defines scientific research as "research applying scientific methods such as technological development and demonstration, fundamental research, applied research and private investment research." Although it borrowed a few phrases from the GDPR,[17] scientific research in the amendment is actually much more widely defined than in the EU. The definition is also somewhat tautological: Is there scientific research that does not apply scientific methods? According to the definition in the amendment, a data controller simply has to claim it is for "scientific research" for pseudonymised personal data to be used and even provided to third parties regardless of the nature of the research.

According to the "reason for proposal" of the amendment, scientific research can include research for "[i]ndustrial purposes, such as the development of new technologies, products and services."[18] However, civil society insists that the range of scientific research should be limited to research that can contribute to the expansion of a society's knowledge based on the publication of the research results. Why should the rights of data subjects be restricted for the private interests of companies? Explaining its personal data protection act that reflected the GDPR, the data protection authority in the United Kingdom, the ICO, said that scientific research "does not apply to processing of personal data for commercial research purposes such as market research or customer satisfaction surveys."[19]

Secondly, the GDPR requires that anonymised, not pseudnonymised data be provided when research can be carried out with anonymous data, but the government amendment has no such provision to minimise the use of personal data as much as possible.

Finally, the amendment excessively restricts the rights of data subjects. In the case of the GDPR, some rights of data subjects can be derogated only when it is not possible to conduct research without such derogation, but the government's amendment limits the rights of data subjects comprehensively. For example, in principle, personal data should be discarded when the purpose of the data collection is achieved, but according to the amendments to the PIPA, pseudonymised data provided to a third party in the name of scientific research can be retained by the recipient indefinitely.

The lack of an independent personal data supervisory authority

A personal data supervisory authority should have multiple powers and be independent for effective supervision. The European Court of Justice (ECJ) has emphasised that a completely independent supervisory authority is "'a guardian' of rights related to the processing of personal data and an essential component for the protection of personal data."[20] Article 52 (Independence) in the GDPR also states that a "supervisory authority shall act with complete independence in performing its tasks and exercising its powers."

The PIPC of Korea was established by the enactment of the PIPA in 2011. Korean civil society has demanded the establishment of an independent

[15] www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0002547315

[16] Chamsesang. (2018). Op. cit.

[17] GDPR recital 159. https://gdpr-info.eu/recitals/no-159

[18] law.nanet.go.kr/download/downloadDB.do?dataCode=bbsBasic&dataSid=23941

[19] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/

[20] Psygkas, A. (2010, 29 March). ECJ C-518/07 – Commission v. Germany: How "independent" should independent agencies be? *Comparative Administrative Law Blog*. https://campuspress.yale.edu/compadlaw/2010/03/29/cases-ecj-c-51807-commission-v-germany-how-independent-should-independent-agencies-be

and fully authorised personal data supervisory authority since before the enactment of the PIPA. However, as mentioned earlier, the Korean supervisory authority, the PIPC, does not have sufficient authority or independence. While it is somewhat positive that the amendment unifies the authorities of the MOIS and KCC into the PIPC, the independence of the integrated PIPC is still limited. This is because the amendment still allows the prime minister to exercise authority to direct and supervise administrative affairs, including the improvement of laws related to the protection of personal data, and the establishment and execution of policies, system and plans. Korean civil society groups are demanding that the PIPC should be guaranteed full independence from the government by excluding the prime minister's authority to supervise.

Conclusion

Civil society fears that if the PIPA amendment is passed as it is, different companies would share, sell and combine customers' data indefinitely. As noted above, companies have consistently sought to combine customers' data with those of other companies. For instance, if this amendment were passed, telecoms could pseudonymise their customers' data and provide this to other companies such as internet service providers and financial companies in the name of research. In this case, the telecom is unlikely to provide the pseudonymised data free of charge, but may require payment or require the other party's personal data sets in return. In addition, through designated public institutions, telecoms and insurance companies would be able to combine pseudonymised customer data. In this way, there is the risk that pseudonymised customer data could be widely shared among numerous companies.

Korean civil society does not oppose the development and utilisation of technologies involving big data, IoT and AI. However, their use should not justify the violation of the rights to informational self-determination of data subjects.

As can be seen in many international reports, these new technologies could increase the risk of discrimination and surveillance as well as privacy violations. Therefore, for the safe development and utilisation of new technologies, the PIPA needs to be overhauled in response to the era of big data and AI. In addition, it is necessary to establish an independent and fully empowered personal data supervisory authority.

For the development of new technologies such as AI, the data subject needs to trust that his or her personal data will be protected. This is an essential factor if new technologies are to be successfully used in reshaping society. Given the fact that personal data is transferred across borders, this issue is also not just a matter for Korea, but a matter that requires global norms and regulations.

Action steps

The following action steps are suggested for South Korea:

- Launch a campaign to inform the public of the problems in the amendment of the PIPA.
- Convince lawmakers to delete the toxic clause that allows reckless commercial use of personal data in the proposed amendment of the PIPA.
- Urge the government and the national assembly to update the PIPA to include safeguards, such as strengthening the need for a privacy impact assessment, regulating profiling and introducing privacy by design and by default in order to protect personal data that is vulnerable in the era of big data and AI.
- Urge the government and the national assembly to ensure that the PIPC can become an independent and fully empowered authority to protect the rights of data subjects.

GLOBAL INFORMATION SOCIETY WATCH 2019

Artificial intelligence:

Human rights, social justice and development

Artificial intelligence (AI) is now receiving unprecedented global attention as it finds widespread practical application in multiple spheres of activity. But what are the human rights, social justice and development implications of AI when used in areas such as health, education and social services, or in building “smart cities”? How does algorithmic decision making impact on marginalised people and the poor?

This edition of Global Information Society Watch (GISWatch) provides a perspective from the global South on the application of AI to our everyday lives. It includes 40 country reports from countries as diverse as Benin, Argentina, India, Russia and Ukraine, as well as three regional reports. These are framed by eight thematic reports dealing with topics such as data governance, food sovereignty, AI in the workplace, and so-called “killer robots”.

While pointing to the positive use of AI to enable rights in ways that were not easily possible before, this edition of GISWatch highlights the real threats that we need to pay attention to if we are going to build an AI-embedded future that enables human dignity.

GLOBAL INFORMATION SOCIETY WATCH
2019 Report
www.GISWatch.org

APC ARTICLE 19 Sida